Personal Data Processing Agreement

Personal Data Processing Agreement for Final Customers of Register Services

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 hereinafter, the details of which are specified below, and Register S.p.A. ("**Register**"); the Client and Register 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. Register 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 the link https://www.register.it/company/legal/?lang=en ("**MSA**") and, in order to provide the aforementioned Service under this DPA, Register 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 Register to comply with, concerning the Processing of Client's Personal Data for the provision of the Service. Accordingly, Register 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 the Data Processor 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. For the purposes of this DPA, the Data Controller is the Client.

"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. For the purposes of this DPA, the Data Processor is Register.

"**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 by sending a written request to dpo@register.it.

"**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: https://www.register.it/company/legal/?lang=en;

"Non-EEA Entity" means any entity, acting as Data Processor (or Sub-processor), Processing Client Personal Data, for the provision of the Service, in a country outside the EEA or a country which has not received an Adequacy Decision.

"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" means the services agreed in the MSA;

"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 from a EU Data Controller to a Non-EEA Entity acting as Data Processor adopted by the European Commission in its Decision 2010/87/UE on 5 February 2010 including its Appendixes 1 and 2 (Annexes 1 and 2 of this DPA) attached hereto.

"Sub-processor" means an entity engaged by Data Processor to assist it in (or who undertakes any) Processing of the Client Personal Data in fulfilment of Data Processor's obligations pursuant to the DPA, as listed in the List of Sub-processors, which has been approved by the Data Controller 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) This DPA applies exclusively where Client acts as the Data Controller regarding Client Personal Data Processed by Register in the provision of the Service;
b) Register acts 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 the Data Processor in the provision of the Service.

3. DATA PROCESSOR'S OBLIGATIONS

3.1. The 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, the Data Processor undertakes to adhere to the following obligations including those defined in Annexes 1 and 2 attached hereto:

a) The Data Processor Processes the Client Personal Data only as necessary to provide the Service, subject to the Data Controller's written instructions in the present DPA;
b) The Data Processor notifies the Data Controller in case it considers a Data Controller's written instruction to breach Applicable Data Protection Laws. In no case is the Data Processor under the obligation of performing a comprehensive legal examination with respect to a Client's written instruction;
c) Register as Data Processor notifies the Data Controller 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 Data Controller and not on the Data Processor;
d) The Data Processor 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 the Data Processor 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 the Data Processor discloses Client Personal Data to its personnel directly and exclusively involved in the performance of the Service, the Data Processor 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 the Data Processor in compliance with its obligations under this DPA.

4. Data Controller's obligations

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

4.2. The Data Controller 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 the Data Processor 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 Register to comply with, concerning the Processing of Client Personal Data for the provision of the Service.

5. Consent to Sub-processing

5.1. The Data Controller 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 the Data Processor or its Sub-processors as described in the List of Sub-processors.

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

a) provides the Data Controller with prior information as to the identity of the Sub-processors as described in the List of Sub-processors and notify the Data Controller of any update in the List of Sub-processors so that the Data Controller 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 Data Controller's request, the Data Processor provides the Data Controller with reasonable information as to actions and measures the Data Processor and its Sub-processors have undertaken to practically comply with the provisions set forth in this DPA.

6. Transfer of Personal Data and incorporation of Standard Contractual Clauses (where applicable)

6.1. To the extent the Regulation is applicable and there are no Adequacy Decisions, the Data Controller and the Data Processor undertake to sign the Standard Contractual Clauses. Moreover, the Data Controller expressly authorises the signature of the Standard Contractual Clauses, allowing the Data Processor to enter the Standard Contractual Clauses with Non-EEA Entities on behalf of the Data Controller.

6.2. Pursuant to Clause 6.1, the Parties acknowledge that Annexes 1 and 2 of this DPA shall apply, and that Annexes 1 and 2 shall be deemed to be Appendixes 1 and 2 of the Standard Contractual Clauses. The Data Processor is authorised by the Data Controller to unilaterally amend Appendixes 1 and 2 of the Standard Contractual Clauses only to the extent they impose stricter obligations on the Non-EEA Entity.

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

6.4. Upon request, the Data Controller may require the opportunity to review the Standard Contractual Clauses, including Annexes 1 and 2.

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

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, the Data Processor assists the Data Controller by appropriate technical and organisational measures for the fulfilment of the Data Controller 's obligation to respond to requests for exercising the Data Subject's Rights.

8.2. The Data Processor will provide Data Controller 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 Data Controller to comply with its duties under Applicable Data Protection Laws in relation to the Data Subject's Rights. The Data Controller acknowledges and agrees that in the event such cooperation and assistance require significant resources on the part of Data Processor, this effort will be chargeable upon prior notice to, and agreement with, the Data Controller.

9. Data return and deletion

9.1. The Data Processor will at no cost to the Data Controller, return or destroy Client Personal Data upon request of the Data Controller and upon the expiration or earlier termination of this DPA subject to a written request of the Data Controller 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 the Data Processor from doing so.

9.2. With respect to specific requests from the Data Controller 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 Register'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 Data Controller opts for the deletion of Client Personal Data and save Art. 9.5, the Data Processor provides a statement assuring such deletion.

9.5. The Data Processor may retain Client Personal Data which is stored in accordance with regular computer back-up operations in compliance with the Data Processor's disaster recovery and business continuity protocols (see Art. 12), provided that the Data Processor 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 the Data Processor 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. The Data Processor will not be responsible for Data Controller'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, the Data Processor may suspend the Data Controller's use of the Service via the Internet immediately pending an investigation, provided that the Data Processor 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 Data Controller in order to continue the provision of the Service via other communication channels.

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

11. Personal Data Breach

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

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

a) take appropriate actions to contain and mitigate such Personal Data Breach, including notifying the Data Controller, without undue delay, to enable the Data Controller to expeditiously implement its response program. Notwithstanding the above, the Data Processor 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 Data Controller 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 Data Controller 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 Data Controller, as Data Controller 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 Data Controller'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 The Data Processor 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 Data Controller upon request. The Data Processor 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 Data Controller explicitly mandates the Data Processor I to carry out on behalf of the Data Controller, the activities described in Art. 5 and 6 above.

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

ANNEX 1 (Appendix 1 to the Standard Contractual Clauses, where applicable)

1. DATA EXPORTER

The Data Exporter/the Controller is: the Data Controller as defined in the Art. 1 of DPA or the Data Processor as authorised by the Data Controller pursuant to Art. 6 of the DPA.

2. DATA IMPORTER

The Data Importer/the Data Processor is: the Data Processor as defined in Clause 1 of the DPA or the Sub-processor as authorised by the Data Controller in Art. 5 and 6 of the DPA.

3. DATA SUBJECTS

The Personal Data transferred/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 acting as Data Controller by using the Service/s provided by Register:

4. CATEGORIES OF PERSONAL DATA PROCESSED FOR EACH SERVICE

The Personal Data transferred/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 acting as Data Controller by using the Service/s provided by Register.

5. SPECIAL CATEGORIES OF DATA

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

6. PROCESSING OPERATIONS

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

ANNEX 2 (Appendix 2 to the Standard Contractual Clauses, where applicable)

Description of the Technical and Organisational Security Measures

The Data Processor and the Sub-processors undertake to maintain no less than the technical and organisational measures described below.

Information on Security Measures

For more details on the security measures of PEC SPID services, please refer to the operating manuals (https://www.register.it/wp-content/uploads/Manuale_Operativo_PEC_Register_it.pdf https://www.register.it/assistenza/manuali-spid/) relating to the aforesaid services drawn up in compliance with the provisions of the Agency for Digital Italy ("Agenzia per l'Italia Digitale").

For the other Services of the Company, security measures are hereby listed:

Information security procedures

Internal organization

Separate roles and responsibilities have been defined for information security and have been assigned to the Company's persons in charge of the Processing activities (hereinafter also "users") in order to avoid conflicts of interest and prevent inappropriate activities.

Human resources security

Mobile devices and teleworking

There is a security Policy for the use of all company devices, in particular mobile devices, and adequate controls are in place.

Conclusion or changes to the employment relationship

Upon the termination of a user's employment from the organisation or in the case of a significant change in the role overtaken, access permissions are updated immediately, while business tools are returned and reset both physically and theoretically.

Management of corporate assets resources

Responsibility of the resources and of company assets

All company tools and assets are carefully inventoried and the allocation of the same to the various users who are responsible for their safety is monitored. A policy has further been defined for their correct use.

Classification of information

All information is classified and catalogued by the respective users in line with the requirements of security, as well as processed appropriately.

Media management

The information stored in the media is managed, controlled, modified and used in such a way as not to compromise its content and is deleted in an appropriate manner.

Access control

Business requirements for access control

The organisational company requirements for monitoring access to information resources are documented in a policy and implemented in practice through an access control procedure; meaning that access to the network and connections is limited.

User access management

Allocation of user access rights is controlled from the user's initial registration until the removal of access rights when they are no longer needed, including special restrictions on privileged access rights and the management of "secret authentication information", and is subject to periodic reviews and checks including an updating of access rights when necessary. In access management, the criterion of minimising access

rights is used, as these are issued in order to grant the user only access to the data that necessary for his job function and business activity. Additional access rights require specific authorisation.

User responsibility

Users are aware of their responsibilities also through the maintenance of effective access control, for example by choosing a complex password, which complexity is verified by the system, and keeping it confidential.

Systems and applications for access control

Access to information is subject to restrictions in compliance with the access control policy, through a system of secure access and access password management as well as control over privileged utilities and limited access to all source codes.

Encryption

Cryptographic control

There is a Policy in place on the use of media encryption and user data. Authentications are encrypted.

Physical and environmental security

Physical and environmental security measures are in place to prevent illegitimate or accidental access, loss or dissemination of data.

Safe areas: data center

The Company's services are provided and hosted in several data centres around the world, which the one storing customers' personal data is among one of the few certified Tier IV in Italy, that is the maximum guarantee that a data centre can offer. All data centres within the supply chain offer complete redundancy of all electrical, cooling and network circuits. All data centres have perimeter lighting as well as a presence detection system with CCTV cameras; the emergency doors are equipped with an alarm. All alarms are concentrated in control rooms.

Physical access is regulated and controlled by authorisation, recognition and registration procedures and is limited, thanks to the access control system, to the areas for which an authorisation exists.

Equipment

There is a policy in place for the disposal of discarded equipment in order to safely destroy all the information thereby contained.

Security of operations

Procedures and operational responsibilities

Operational responsibilities in IT are documented and changes to IT facilities and systems are controlled. Development systems, verification systems and operational systems are separate. There are users who are responsible for the proper functioning of the procedures. On the other hand, the management of the logical security of the operating systems and of the applications installed by the customer is the responsibility of the customer of the individual services provided by the Company (hereinafter also the "customer").

Protection against malware

Viruses and malware control is active on company devices, and there is an appropriate awareness from the users.

With regard to the services of Virtual Server or Dedicated Server, the customer is responsible for installing anti-virus and anti-malware software and - if the related service has not been purchased - of a firewall. With regard to the Hosting service, a real-time protection on the front-end machines is in place.

With regard to the e-mail service, mail traffic is analysed in real time, both incoming and outgoing, for the detection of viruses, malware and for the identification and filtering of spam. The analysis is automated and is based on the nature of the content, on the interrogation of international databases, and on the reputation acquired due to a series of parameters.

Backup

Periodic backups are performed, with the exclusion of services for which the customer is responsible for maintaining and managing backups (Dedicated Servers and Virtual Servers). For Hosting and Post services, periodic backups are performed which, for Hosting services, can also be accessed by the customer. Additional backups, not accessible by customers, are carried out for the sole purpose of Disaster Recovery.

Authentication and monitoring

Authentication and synchronization
Every activity and event related to the security of information by system users and administrators / operators occurs after entering the authentication credentials or certificates of identity. The clocks of all the equipment are synchronised.
Control of operational software
Software installation on operating systems is controlled and monitored.

With regard to Virtual Servers and Dedicated Servers, operating systems released to customers are made available with updated installation images even during installation by the customer. It is also the customer's responsibility to update the firmware and the applications or software installed by the customer.

Management of technical vulnerabilities
Patch management
Each technical vulnerability is corrected with appropriate patches and procedures are provided for all the test phases and for the subsequent installation of the software and updates, which takes place only when all the tests are positive.
Information systems audit considerations
Periodic checks are performed in order to check that any negative effect on production systems is minimised and that there is no unauthorised access to the data.

Security of communications
Network security management
Networks and online services are also secured through their separation and segregation.
Transfer of information
Agreements regarding the transfer of information to and from third parties are in force.

Acquisition, development and maintenance of the system
Security in development and support processes
The rules that govern the security of software and system development are defined in a Policy. Changes to the system (both for applications and for operating systems) are controlled. System security is tested and eligibility criteria which include security aspects are defined.

Relationship with suppliers
Information security in the relationship with suppliers
There are contracts or agreements aimed at protecting and regulating the Processing of information of the organisation and of the customers that are accessible to third parties operating in the IT area and to other third-party suppliers that are part of the entire supply chain.
Management of services rendered by the supplier
The provision of services rendered by suppliers is monitored and verified in relation to the contract or agreement. Every change to the service is checked.

Incident management for safety information
Information security incidents management and improvements
There are specific responsibilities and procedures aimed at managing in coherence and effectively all events and incidents relating to information security (e.g. the so-called Data Breach procedure).

Information security aspects related to business continuity
Redundancies
All major IT facilities are redundant in order to meet availability requirements. Where this redundancy is not in place, adequate measures are in place to ensure continuity of service or minimisation of data loss.

Compliance

Compliance with legal and contractual requirements

The company identifies and documents its obligations to external authorities and other third parties in relation to information security, including intellectual property, accounting documentation and privacy information.

Review of information security

The organisation's projects relating to information security and security policies are revised and corrective actions are taken where necessary.

ANNEX 3

Annex 3 (List of sub-processors) must be asked by e-mail to: dpo@register.it.

Personal Data Processing Agreement for Clients who request Register's Services on behalf of third parties

II. PREAMBLE

Whereas:

A. The Client, with regards to the services provided to its customers, generally acts as a Data Processor – where these customers, as the case may be, will act as Data Controllers or Data Processors themselves.

B. In the context of the provision of these services, the Client may engage sub-processors to provide those services on its behalf. Where the Client acts as a Data Processor, these sub-processors will also be considered Data Processors, under Reg. (EU) 2016/679 (hereinafter: "**GDPR**").

C. The Client wishes to regulate its relationships with its sub-contractors, by means of a written agreement in line with the requirements of Art. 28 GDPR.

D. This Personal Data Sub-Processing Agreement, together with its Annexes, (collectively, the "**DSPA**") is entered into between the Client (hereinafter: "**Client**" or "**Processor**"), namely the natural person or legal entity which requested the Service, as defined hereinafter, on behalf of third parties in order to resell it or not, and Register S.p.A. (hereinafter: "**Sub-Processor**" or "**Register**"); the Client and Register, collectively referred to as "**Parties**", and each one individually as "**Party**, enter into this DSPA in order to reflect the Parties' agreement related to the Processing of Personal Data in relation with the Service ("**Client Personal Data**"), in accordance with the requirements of the Applicable Data Protection Laws.

E. Register has agreed to provide the service/services to the Client ("**Service**"), under the terms of the agreement entered into the Service Order and the General Conditions and Service available via the link https://www.register.it/company/legal/?lang=en (hereinafter: "**Master Agreement**").

F. The subject-matter, nature and purpose of the Processing of Client Personal Data related to the Service, as well as the type of Personal Data and categories of Data Subjects concerned, are fully described in Annex 1 of this DSPA.

G. The Parties have entered into this DSPA in order to ensure that they comply with the Applicable Data Protection Laws and so as to establish safeguards and procedures for the lawful Processing of the Client's Personal Data.

The above preamble forms an integral part of this DSPA.

1. DEFINITIONS

1.1. Unless otherwise defined in this DSPA, all terms in capital letters used in this DSPA will have the meaning given to them in the Master Agreement. In the event of any conflict or inconsistency in terms of data protection safeguards between this DSPA and the Agreement, this DSPA 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: in EU Member States, the Regulation and complementary national data protection laws, including any guidance and / or codes of practice issued by the relevant Supervisory Authorities within the EU; in non-EU countries, any applicable data protection laws regarding safeguarding and lawful Processing of Personal Data;

Client Personal Data: Personal Data, relating to Data Subjects, Processed in connection with the Service;

Data Controller: 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: in general, a natural or legal person, public authority, agency or other body which Processes Personal Data on behalf of the Data Controller;

Data Subject: has the meaning set forth in the GDPR;

Data Subjects' Rights: the rights which Data Subjects are entitled to under the Applicable Data Protection Laws. To the extent that the GDPR is applicable, **Data Subjects' Rights** include, e.g., the right to request access to, rectification or erasure of Personal Data, to request the restriction of Processing concerning the Data Subject or to object to Processing, as well as the right to data portability, from the Data Controller;

DSPA: this Data Sub-Processing Agreement, together with its Annexes;

EEA: means the European Economic Area.

GDPR: 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;

List of Sub-Processors: indicates the available list by sending a written request to dpo@register.it;

Master Agreement: indicates 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: https://www.register.it/company/legal/;

Non-EEA Entity: means any entity, acting as Data Processor (or Sub-processor), Processing Client Personal Data, for the provision of the Service, in a country outside the EEA or a country which has not received an Adequacy Decision.

Personal Data: 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. For the avoidance of doubt, **Personal Data** has the meaning as set forth in the GDPR and the Applicable Data Protection Laws;

Personal Data Breach: 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;

Process or **Processing:** any operation, or set of operations, which is performed on Personal Data, or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Processor: generally, refers to the natural or legal person, public authority or other entity that handles Personal Data on behalf of the Controller. For the purposes of this DSPA, the Processor is the Client and the Sub-Processor is Register S.p.A.;

Service: the service described in the Master Agreement;

Special Categories of Personal Data: Personal Data that reveals: racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership of natural persons, as well as genetic data, biometric data (when Processed 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 from a EU Data Controller to a Non-EEA Entity acting as Data Processor adopted by the European Commission in its Decision 2010/87/UE on 5 February 2010 including its Appendixes 1 and 2 (Annexes 1 and 2 of this DPA) attached hereto.

Sub-Processor: entity identified by the Processor to assist in (or directly undertake any) Processing of Client Personal Data in compliance with the obligations set by the Processor and referred to in this DSPA;

Supervisory Authority: any authority which has powers to monitor and enforce the application of the Applicable Data Protection Laws regarding the Processing of Client Personal Data in the context of the provision of the Service.

2. DATA PROTECTION ROLES

2.1. The Parties agree that:

a) This DSPA exclusively applies to the cases where the Client and Register are both Data Processors regarding Client Personal Data Processed in the context of the provision of the Service;

b) The clients to which the Service is to be provided may act as Data Controllers, or as Data Processors on behalf of Data Controllers (e.g., these clients' end users);

c) Register has been engaged by the Client to provide the Service, on its behalf, to its clients;

d) This DSPA governs the relationship between the Parties in terms of respective duties and obligations concerning the Processing of Client Personal Data by the Sub-Processor in the context of the provision of the Service.

3. SUB-PROCESSOR'S OBLIGATIONS

3.1. Sub-Processor commits to complying with the following obligations, including those defined in Annexes 1, 2 and 3 which are considered an integral part of this DSPA:

a) Sub-Processor will Process Client Personal Data only as necessary to provide the Service and subject to the Client's written instructions, including as provided in the Agreement and this DSPA;
b) Sub-Processor will notify the Client in the event that it considers a specific written instruction that was received, to be in violation of the Applicable Data Protection Laws;
c) Sub-Processor will notify the Client without undue delay of any contact, communication or correspondence it may receive from a Supervisory Authority, related to the Processing of Client Personal Data;
d) Sub-Processor has implemented adequate operational, technical and organisational measures under Art. 32 GDPR to protect the Client Personal Data. The Parties are aware and agree that the Sub-Processor is expressly authorized to implement alternative measures or to establish alternative places of data retention provided the level of security of the measures or places chosen is considered, in all respects, adequate;
e) In the event that the Sub-Processor discloses Client Personal Data to its personnel which is directly and exclusively involved in the provision of the Service, Sub-Processor will ensure that such personnel:
   i) is committed to confidentiality or is under an appropriate statutory obligation of confidentiality; and
   ii) Processes Client Personal Data under the instructions of Sub-Processor, and in compliance with Sub-Processor's obligations under this DSPA.

4. COOPERATION AND ACCOUNTABILITY OBLIGATIONS

4.1. The Parties will cooperate in good faith, in order to ensure compliance with the provisions of this DSPA and to assist the Data Controllers in complying with their obligations under the Applicable Data Protection Laws, including, but not limited to, assuring the correct and timely exercise of Data Subjects' Rights, managing incidents in the event of a security / Personal Data Breach so as to mitigate their possible adverse effects.

4.2. The Parties will cooperate in good faith, in order to make available to the Data Controllers and to each other, as well as to Supervisory Authorities, all information necessary to demonstrate compliance with the Applicable Data Protection Laws.

4.3. The Sub-Processor must allow for and contribute to audits, including inspections, conducted by the Client, the Data Controllers or auditors mandated by the Client or the Data Controllers, on Sub-Processor's systems and locations used to Process Client Personal Data. Audits or inspections carried out must be preceded by reasonable prior notice to the Sub-Processor and must not interfere with the normal business operations of the Sub-Processor. Any information gathered on the Sub-Processor's activities will be held in conditions of strict confidentiality, except where mandatory applicable laws (including, but not limited to, the Applicable Data Protection Laws) or binding orders from law enforcement authorities (including, but not limited to, the Supervisory Authority) require information to be disclosed.

5. PERSONAL DATA PROCESSING AUTHORIZATION BY FURTHER SUB-PROCESSORS

5.1. The Client acknowledges, agrees and consents that, for the sole purpose of proceeding with the provision of the Service and in compliance with the provisions of this DSPA, the Client Personal Data may be processed by additional sub-processors, as described in the List of Sub-Processors.

5.2. Pursuant to art. 5.1, Register is authorized to use additional sub-processors, provided that:
a) it informs the Processor of the identity of the sub-processors in advance, as described in the List of sub-processors and notifies the Processor of any update of the aforementioned list in order to allow the Processor to oppose the introduction of the said sub-processors;

b) it signs agreements with sub-processors that contain the same obligations as those set forth in this DSPA regarding the Processing of the Client's Personal Data;
c) it exercises adequate controls in selecting the sub-processors and remains responsible for the fulfilment of the obligations contained in the present DSPA by the sub-processors involved;
d) at the request of the Processor, the Sub-Processor provides the Processor with adequate information regarding the actions and measures that the Sub-Processor and its additional sub-processors have undertaken to ensure compliance with the provisions of this DSPA.

6. TRANSFER OF PERSONAL DATA AND MANDATE TO EXECUTE THE STANDARD CONTRACTUAL CLAUSES (WHERE APPLICABLE)

6.1. Depending on the Services activated by the Client, pursuant to Art. 5.1 and 5.2, Register may transfer Client Personal Data to one or more further Sub-Processors who are Non-EEA Entities and Data Importers for the purpose of the Standard Contractual Clauses. Where there are no Adequacy Decisions applicable to the Non-EEA Entity, Register and the Client enter into the Standard Contractual Clauses attached to this DSPA.

6.2. For the purpose of entering into the Standard Contractual Clauses pursuant to Art. 6.1, Register warrants to act on behalf of the Non-EEA Entity (Data Importer) pursuant to a valid mandate, while the Client similarly guarantees to act on behalf of the Data Controller (Data Exporter) pursuant to a valid mandate.

6.3. Register and the Client are aware that Annexes 1 and 2 of this DSPA shall apply, and that Annexes 1 and 2 shall be considered Appendixes 1 and 2 of the Standard Contractual Clauses.

6.4. Nothing within this DSPA may prevail over any clause within the Standard Contractual Clauses.

6.5. Upon request, the Client may revise the Standard Contractual Clauses entered into between Register and the Non-EEA Entity, thereby also including Appendixes 1 e 2.

6.6. The Client is aware that it is the responsibility of the Data Controller to respect every task and obligation which may be applicable in order to enable the lawful transfer of Client Personal Data to Non-EEA Entities for the purposes of Applicable Data Protection Laws.

7. DATA SUBJECTS' RIGHTS

7.1. Taking into account the nature of the Processing, the Sub-Processor will assist the Client in the fulfilment of the Client's obligation to assist Data Controllers in responding to requests to exercise Data Subjects' Rights, by means of appropriate technical and organisational measures.

7.2. The Sub-Processor will cooperate with and assist the Client, to a reasonable extent, and will provide to the Client such information as may reasonably be required to enable Data Controllers to comply with its duties related to Data Subjects' Rights under the Applicable Data Protection Laws.

8. DATA RETURN AND ERASURE

8.1. Without prejudice to Art. 8.5., the Sub-Processor, without placing additional costs charged to the Client, will, upon request, return the Client Personal Data (deleting all copies of the Client Personal Data that is in the Sub-Processor's possession), or will delete the Client Personal Data, without undue delay and no later than Thirty (30) days from the receipt of the Client's request.

8.2. Without prejudice to Art. 8.5., upon expiration or earlier termination of this DSPA, the Sub-Processor, at no cost for the Client, will return the Client Personal Data to the Processor, (deleting all copies of the

Client Personal Data that is in the Sub-Processor's possession), without undue delay and no later than Thirty (30) days from the expiration or earlier termination of this DSPA, unless otherwise requested by the Client.

8.3. Art. 8.1. and Art. 8.2. will not apply where mandatory applicable laws (including, but not limited to, the Applicable Data Protection Laws) or binding orders from law enforcement authorities (including, but not limited to, the Supervisory Authority), prevent the Sub-Processor from complying with them. The Sub-Processor must notify the Client of such circumstances, providing adequate justification and reasoning regarding its legal obligation to retain the Client Personal Data, without undue delay and no later than ten (10) days from receipt of Client's request, or the expiration or earlier termination of this DSPA (as the case may be). The Sub-Processor will remain bound to the terms of this DSPA (even after its expiration or earlier termination) regarding any Client Personal Data kept under the terms of this Article and must not actively or intentionally Process such Client Personal Data for any other purpose other than to comply with the mentioned legal obligations or binding orders.

8.4. Whenever Client Personal Data is returned to the Client (with all copies of the Client Personal Data in Sub-Processor's possession being deleted) or deleted at the Client's request, under the terms of Art. 8.1. or Art. 8.2., the Sub-Processor will provide a statement to the Client assuring such a return and / or deletion without undue delay, and no later than Thirty (30) from the date on which the return and / or deletion is carried out.

8.5. The Sub-Processor may retain the Client Personal Data which is stored in accordance with regular computer back-up operations, in compliance with the Sub-Processor's disaster recovery and business continuity protocols, provided that the Sub-Processor, and any of its sub-processors, may not actively or intentionally Process such Client Personal Data for any purpose other than to provide the Service. The Sub-Processor will remain bound by the terms of this DSPA (even after its expiration or earlier termination) regarding any Client Personal Data kept under the terms of this Clause.

9. PERSONAL DATA BREACH

9.1 If the Sub-Processor becomes aware of a Personal Data Breach, it will:

a) take appropriate actions to contain and mitigate the Personal Data Breach, including notifying the Client without undue delay from the moment after the Sub-Processor becomes aware of the Personal Data Breach;

b) cooperate with the Client and/or Data Controllers to investigate the nature, categories and approximate number of affected Data Subjects, the categories and approximate number of affected Personal Data records and the likely consequences of a Personal Data Breach, in a manner which is commensurate with its seriousness and its overall impact on the Data Controllers and the provision of the Service under the Master Agreement;

c) where the Applicable Data Protection Laws require that the Personal Data Breach be notified to relevant Supervisory Authorities and affected Data Subjects, defer and take instructions from the Client and/or the Data Controllers, to the extent in which Client Personal Data is involved in the Personal Data Breach – the Data Controllers are exclusively entitled to determine the measures to be taken in order to comply with the Applicable Data Protection Laws or to remediate to any risks, including, without limitation:

iii. whether notice is to be provided to any individuals, regulators, law enforcement agencies, consumers' reporting agencies, or others, as may be required by the Applicable Data Protection Laws, or at the Data Controllers' discretion; and

iv. the contents of such a notice, whether any type of remediation may be offered to affected Data Subjects under the Data Controllers' responsibility, and the nature and extent of any such remediation.

10. DISASTER RECOVERY AND BUSINESS CONTINUITY

10.1. The Sub-Processor adopts and updates, according to professional diligence criteria, disaster recovery and business continuity protocols which differ according to the Service and of which a summary is available to the Processor upon request. The Sub-Processor may modify this program at any time, provided that its capacity to cope with disaster recovery is not reduced to a lower level than that envisaged by the aforesaid program at the time of signing this DSPA.

STANDARD CONTRACTUAL CLAUSES

Commission Decision C(2010)593

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Name of the data exporting organisation: the Data Controller, as represented by the Client under Art. 6 of the DSPA

(the data **exporter**)

And

Name of the data importing organisation: the Non-EEA Entity who acts as a further sub-processor of Register, under Art. 5 of the DSPA

(the data **importer**)

each a "party"; together "the parties",

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

(a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject'* and *'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data[1];

(b) '*the data exporter*' means the controller who transfers the personal data;

(c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

(d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

(e) '*the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;

(f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

(a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

(b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

(c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

(d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

(e) that it will ensure compliance with the security measures;

(f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

(g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

(h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

(i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

(j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer[2]

The data importer agrees and warrants:

(a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

(c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

(d) that it will promptly notify the data exporter about:

(i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,

(ii) any accidental or unauthorised access, and

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, *inter alia,* internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

(iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

(e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

(f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

(g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

(h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;

(i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;

(j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

   The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

   (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

(b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely the law which governs the contract or other legal act under Union or Member State law, entered into between the Client and the Data Controller pursuant to article 28, paragraph 3 of Regulation (EU) 2016/679.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses[3]. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.

2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the

---

[3] This requirement may be satisfied by the subprocessor co-signing the contract entered into between the data exporter and the data importer under this Decision.

data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely the law which governs the contract or other legal act under Union or Member State law, entered into between the Client and the Data Controller pursuant to article 28 paragraph 3 of Regulation (EU) 2016/679.

4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

ANNEX 1 (Appendix 1 to the Standard Contractual Clauses, where applicable)

1. DATA SUBJECTS

Client Personal Data which may be Processed, depending on the specifically activated Service, may pertain to 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 acting as Data Controller by using the Service/s provided by Register:

2. CATEGORIES OF PERSONAL DATA

Personal Data which are Processed for any Service provided to the Client, not determinable in advance, exclusively pertain to Personal Data in the meaning set forth in Art. 4 (1) of the Regulation, **excluding in any case 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:

- contact details (name and surname, e-mail address, postal address, phone number)
- date of birth
- age
- gender
- further categories of Personal Data Processed by the Client acting as Data Controller through the Service/s provided by Register:

3. SPECIAL CATEGORIES OF DATA (IF APPLICABLE)

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

4. PROCESSING OPERATIONS

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

ANNEX 2 (Appendix 2 to the Standard Contractual Clauses, where applicable)

Description of the Technical and Organisational Security Measures

The Sub-Processor undertakes to maintain no less than the technical and organisational measures as described hereinafter.

Organization of information security

Internal organization

The organization defines the roles and responsibilities for information security and allocate them to authorized persons of the processing of personal data in order to avoid conflicts of interest and prevent inappropriate activities.

Human resource security

Mobile devices and teleworking

There is a security Policy for the use of all company devices, in particular mobile devices, and adequate controls are in place.

Termination and change of employment

Upon exit of a user from the organization or in the case of a significant change in the role covered, access permissions are updated immediately, the business tools returned and reset both physically and logically.

Asset management

Responsibility for assets

All information assets are inventoried, and owners are identified to be held accountable for their security. 'Acceptable use' policies is defined.

Information classification

Information are classified and labelled by its owners according to the security protection needed,and handled appropriately.

Media handling

Information storage media are managed, controlled, moved and disposed of in such a way that the information content is not compromised.

Access control

Business requirements of access control

The organization's requirements to control access to information assets are clearly documented in an access control policy and procedures. Network access and connections should be restricted.

User access management

The allocation of access rights to users is controlled from initial user registration through to removal of access rights when no longer required, including special restrictions for privileged access rights and the management of passwords and regular reviews and updates of access rights take place. In access management, the criterion of minimizing access rights is used, which are issued in order to allow the user access to the data necessary for his activity. Additional access rights require specific authorization.

User responsibilities

Users are made aware of their responsibilities towards maintaining effective access controls e.g. choosing strong passwords and keeping them confidential.

System and application access control

Information access is restricted in accordance with the access control policy through secure log-on, password management, control over privileged utilities and restricted access to program source code.

Cryptography

Cryptographic controls

There is a policy on the use of media encryption and user data. Authentications are encrypted.

Physical and environmental security

Physical and environmental security measures are in place to prevent illegitimate or accidental access, loss or dissemination of data in the various facilities.

Secure areas: data center

The Company's services are provided and hosted in multiple data centers worldwide. All data centers within the supply chain offer complete redundancy of all electrical, cooling and network circuits. All data centers have a presence detection system with CCTV cameras. All alarms are concentrated in the control room.
Physical access is regulated and controlled by authorization and recognition procedures.

Equipment

A policy is in place for the disposal of discarded equipment in order to safely destroy all the information contained.

Operations security

Procedures and operational responsibilities

Operational responsibilities in IT are documented and changes to IT facilities and systems are controlled. Development systems, verification systems and operational systems are separate. Users are defined as responsible for the proper functioning of the procedures. Instead, it is the responsibility of the customer of the individual services of the Company (hereinafter also the "customer") the management of the logical security of the operating systems and of the applications installed by the customer.

Protection against malware

The control of viruses and malware is active on company devices, and there is an appropriate awareness on the part of users.
With regard to the services of Virtual Server or Dedicated Server, the customer is responsible for installing anti-virus and anti-malware software and - if the related service has not been purchased - of a firewall.
With regard to the Hosting service, a real-time protection on the front-end machines is instead in place.
With regard to the e-mail service, mail traffic is analyzed in real time, both incoming and outgoing, for the detection of viruses, malware and for the identification and filtering of spam. The analysis is automatic and is based both on the nature of the content, both on the questioning of international databases, and on the reputation acquired thanks to a series of parameters.

Backup

Periodic backups are performed, with the exception of services for which the customer is responsible for maintaining and managing backups (Dedicated Servers and Virtual Servers). For the Hosting and Post services, periodic backups are performed which, for Hosting services, can also be accessed by the customer. Additional backups, not accessible by customers, are carried out for the sole purpose of Disaster Recovery.

Logging and monitoring

Logging and synchronization

Every activity and event related to the security of information by system users and administrators / operators occurs after entering the authentication credentials or certificates of identity. The clocks of all the equipment are synchronized.

Control of operational software

Software installation on operating systems is monitored and controlled.

Communications security

Network security management

Networks and network services are secured, for example by separation and segregation.

Information transfer

There are policies, procedures and agreements concerning information transfer to/from third parties.

System acquisition, development and maintenance

Security in development and support processes

The rules that govern the security of software and systems development are defined in a Policy. Changes to the system (both for applications and for operating systems) are controlled. System security is tested and eligibility criteria are defined that include security aspects.

Supplier relationships

Information security in supplier relationships

There are policies, procedures, awareness etc. to protect the organization's information that is accessible to IT outsourcers and other external suppliers throughout the supply chain, agreed within the contracts or agreements.

Supplier service delivery management

Service delivery by external suppliers are monitored and reviewed/audited against the contracts/agreements. Service changes are controlled.

Information security incident management

Management of information security incidents and improvements

There are specific responsibilities and procedures aimed at coherently and effectively managing events and incidents relating to information security (eg the so-called Data Breach procedure).

Information security aspects of business continuity management

The company identifies and documents its obligations to external authorities and other third parties in relation to information security, including intellectual property, accounting documentation and privacy information.

Review of information security

The organization's projects relating to information security and security policies are revised and corrective actions are promoted where necessary.

ANNEX 3 (List of Sub-processors)

Annex 3 (List of Sub-Processors) may be requested to dpo@register.it.