Personal Data Processing Agreement

Personal Data Processing Agreement

Preamble

Whereas:

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

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

C. This Data Processing Agreement, in conjunction with its Annexes, (collectively "**DPA**") is entered into between the Client (hereinafter: "**Client**"), namely the natural person or legal entity which purchased the Service (as defined below) and the details of which are specified below, and 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.

H. The present document, once having been downloaded, shall be filled in, undersigned by the Client, and sent to dpo@register.it, where it will also be undersigned by Register, and, subsequently shall fully replace the 'Personal Data Processing Agreement for final customers of Register's Services' and the 'Personal Data Processing Agreement for Clients who requested Register's Services on behalf of third parties' cited in Article 'Processing of Personal Data' in the General Conditions of Service, since it enables the Client to further identify certain elements of the processing of personal data performed by Register as a Data Processor.

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 Register to the Client.

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

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

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

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

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

"Data Subject's Rights" means the rights recognised to the Data Subject pursuant to the Applicable Data Protection Laws. To the extent the Regulation is applicable, "Data Subject's Rights" means, e.g., the right to request from the Data Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability.

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

"EEA" means the European Economic Area.

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

"**List of Sub-processors**" means the list available 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 to the following link: https://www.register.it/company/legal/?lang=en.

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

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

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

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

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

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

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

"Services Involving Non-EEA Sub-processors" means the "SITELOCK PREMIUM HTTPS" service, which service order may be found here: https://www.register.it/company/legal/ods-sitelock/, as well as the "Micro Site, Simply Site e Simply Shop" service, which service order may be found here: https://www.register.it/company/legal/ods-simplysite/.

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

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

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

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

2. DATA PROTECTION ROLES

2.1. The Parties agree that:

a) The Client is the Data Controller of the Client Personal Data, except if and when the Client acts as the Data Processor of the Client Personal Data on behalf of a third-party which acts as Data

Controller or as Data Processor itself. The Client, or the relevant Data Controller, determines the purposes of the collection and processing of the Client Personal Data;

b) Register acts, in any case, as the Data Processor of the Client Personal Data for the provision of the Service; and

c) this DPA regulates the relationship between the Parties in terms of respective duties and obligations concerning the Processing of Client Personal Data by Register, acting as Data Processor in the provision of the Service.

3. REGISTER'S OBLIGATIONS

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

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

a) Register Processes the Client Personal Data only as necessary to provide the Service, subject to the Client's written instructions in this DPA;

b) Register notifies the Client in case it considers a Client's written instruction to breach Applicable Data Protection Laws. In no case is Register under the obligation of performing a comprehensive legal examination with respect to a Client's written instruction;

c) Register as Data Processor notifies the Client without undue delay of any contact or communication it receives from a Supervisory Authority in relation to the Processing of Client Personal Data. In this regard, the Parties acknowledge and agree that the responsibility for replying to such requests rests on the Client and not on Register;

d) Register 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 Register 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 Register discloses Client Personal Data to its personnel directly and exclusively involved in the performance of the Service, Register 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 Register in compliance with its obligations under this DPA.

4. CLIENT'S OBLIGATIONS

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

4.2. The Client represents and warrants that:

a) it has an appropriate legal basis (e.g., Data Subject's consent, legitimate interests, authorisation from the relevant Supervisory Authority, etc.) to Process and disclose the Client Personal Data to Register 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 Client acknowledges, agrees and consents that, for the sole and exclusive purpose of delivering the Service and subject always to compliance with the terms of this DPA, Client Personal Data may be Processed by Register or its Sub-processors as described in the List of Sub-processors.

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

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

6. TRANSFER OF PERSONAL DATA

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

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

6.3. Upon request, the Client may require the opportunity to review the Standard Contractual Clauses. To the extent necessary to protect business secrets or other confidential information, including Personal Data, Register may redact part of the text of the Standard Contractual Clauses prior to sharing a copy.

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

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

(i) Clause 7 of the Standard Contractual Clauses is applicable;
(ii) Only the clauses of the Standard Contractual Clauses under MODULE FOUR: Transfer processor to controller apply (to the exclusion of the other MODULES).
(iii) Clauses 14 and 15 do not apply, considering that the Services do not entail the combination of the Client Personal Data received from the Non-EEA Controller with other Personal Data collected by Register in the EU.
(iv) Under Clause 17 of the Standard Contractual Clauses, Option 2 is applicable. The laws of Italy will apply.
(v) Under Clause 18 of the Standard Contractual Clauses, the courts of Florence (Italy) will apply.
(vi) Only Annex 1 of this DPA will apply and it will be deemed as Annex I of the Standard Contractual Clauses.

7. COOPERATION AND ACCOUNTABILITY OBLIGATIONS

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

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

8. DATA SUBJECT RIGHTS

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

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

9. DATA RETURN AND DELETION

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

9.2. With respect to specific requests from the Client for a return of the Client Personal Data, such request will be met to the extent feasible, subject to the provisions of the applicable service order (link) and to the technically and organisationally reasonable commercial 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 Client opts for the deletion of Client Personal Data and save Art. 9.5, Register provides a statement assuring such deletion.

9.5. Without prejudice to the provisions of article 9.2. above, Register may retain Client Personal Data which is stored in accordance with regular computer back-up operations in compliance with Register's disaster recovery and business continuity protocols (see Article 12), in accordance with article 32 of the Regulation, provided that Register 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 Register 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. Register will not be responsible for Client's access to the Internet, for any interception or interruption of any communications through the Internet, or for changes to or losses of Personal Data through the Internet.

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

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

11. PERSONAL DATA BREACH

11.1 The Client acknowledges and agrees that Register shall not be deemed responsible for Personal Data Breach not imputable to Register's negligence.

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

a) take appropriate actions to contain and mitigate such Personal Data Breach, including notifying the Client, without undue delay, through channels that may include certified e-mail (PEC), to enable the Client to expeditiously implement its response program. Notwithstanding the above, Register reserves the right to determine the measures it will take to comply with Applicable Data Protection Laws or to protect its rights and interests;

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

c) where Applicable Data Protection Laws require notification to relevant Supervisory Authorities and impacted Data Subjects of such a Personal Data Breach, and as it relates to the Client Personal Data, defer to and take instructions from Client, as 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 Client's discretion; and

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

12. DISASTER RECOVERY AND BUSINESS CONTINUITY

12.1 Register maintains commercially reasonable disaster recovery and business continuity protocols, which differ between each Service provided, a copy of the summary of which is available for review by the Client upon request. Register may amend such plan at any time, provided that it shall not reduce its disaster recovery ability to less than the disaster recovery ability in effect pursuant to such plan as in existence on the effective date.

13. MANDATE

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

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

The Client	Register S.p.A.
Name and surname / name of the company _____	
C.F. / P. IVA _____	VAT NUMBER 04628270482
Date and Place _____	Florence, _____
(Signature) _____	(Signature) _____

ANNEX 1

1. DATA SUBJECTS

The Personal Data Processed concern the following categories of Data Subjects (mark with an X):

☐ clients and/or potential client

☐ providers

☐ employees and/or potential employees

☐ advisors and/or professionals

☐ other (please specify):

_____

2. CATEGORIES OF PERSONAL DATA PROCESSED FOR EACH SERVICE

The Personal Data Processed concern the following categories of data (mark with an X):

☐ data of contact (name and surname, e-mail address, postal address, phone number)

☐ date of birth

☐ age

☐ sex

☐ other (please, specify):

_____

3. SPECIAL CATEGORIES OF DATA

The Personal Data Processed concern the following special categories of data (mark with an X):

☐ disabilities and/or accidents

☐ political opinions

☐ religious or philosophical beliefs

☐ sex life or sexual orientation including the relationship or conjugality

☐ trade union membership

☐ health state and/or illness

☐ criminal convictions and arrests

☐ other (please specify):

_____

4. PROCESSING OPERATIONS

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

5. NATURE OF THE PROCESSING

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

6. FREQUENCY OF THE PROCESSING

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

7. DURATION OF THE PROCESSING

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

ANNEX 2

Description of the Technical and Organisational Security Measures

Register 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 (subject to the provisions of the applicable service order (link). 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.