SUPPLHI

Adaptive SRM

SupplHi SRM SaaS - Standard T&C and DPA for Vendors

[English]

PUBLIC

www.supplhi.com

[ENG] Standard Terms and Conditions for the use of the SRM SaaS by “Vendors”

The following Terms and Conditions apply to all users registered with a "Vendor" profile (i.e. organizations that may supply goods and/or services to users of “Buyer” organizations).

The "Buyer" profile (i.e. organizations to which SupplHi provides access to the platform for managing their own supplier base) has its own dedicated Terms and Conditions.

Our mission

SupplHi is the cloud-based Software-as-a-Service (SaaS) Supplier Relationship Management (SRM) platform for B2B supplies of goods and services. Our mission is to enable every organization to grow through its supply chain. SupplHi, in fact, enables Buyer organizations to carry out their supplier base management processes efficiently and in compliance with applicable regulations, in light of international market best practices - bringing order through controlled SRM processes and easy access to information, without wasting a single moment of their time.

SupplHi makes its digital infrastructure available to the B2B world with the aim of increasing efficiency, reducing costs and creating greater opportunities for Buyer and Vendor organizations globally.

All data on the SupplHi platform (forms, attachments, information, e-mails) is stored in highly reliable structures and on hosting located in the European Union (currently in Ireland) on Amazon Web Services (AWS).

It is also possible to use our marketing website by browsing as a Visitor. In this case, login is not required, but it is not possible to access all the content and functionalities of the platform. When you use the services we offer, you become part of our network and undertake to use our site responsibly and to comply with its rules of use.

Agreement

By registering on our site you enter into an agreement with SupplHi S.r.l. Società Unipersonale, Via A. Calabiana, 6 - 20139 Milan, Italy, registered with the Milan Chamber of Commerce (C.C.I.A.A.) under number 09721660968, R.E.A. MI 2110015, with Tax Code and VAT Number 09721660968, info@supplhi.com (hereinafter simply "SupplHi") and you accept all of the following terms on your own behalf or on behalf of the company you represent. This agreement also governs the use of mobile applications.

If your company has authorized you to act as its representative, you are entering into this agreement on behalf of your company. You are both subject to the rules set out in this agreement. If you are not authorized, you are personally bound by this agreement. By using our website, you confirm that you are at least 18 years old and that you have the right to enter into this agreement.

Protection of personal data

Any processing of personal data is carried out by SupplHi to provide the requested service in its capacity as processor, as defined in Article 4(1)(8) of General Data Protection Regulation 2016/679, in compliance with the provisions set out in the Data Protection Agreement.

Service

SupplHi's role is to provide Buyer organizations - through the SaaS platform - with access to structured and constantly updated information on Vendors, so that they can independently manage their own Supplier Relationship Management (SRM) processes. For example, SupplHi does not decide whether a given Vendor is qualified or not, either within the network of Buyer organizations using the platform or in relation to a specific Buyer organization, and the decision to qualify a Vendor always remains with the individual Buyer organization.

As part of the provision of services to Buyer organizations and based on the modules and functionalities selected and configured for each specific Buyer organization, SupplHi offers the following free Services to Vendors:

- Managing, for each Vendor (whether a company or a natural person) - through identification codes defined by SupplHi on a national basis (VAT, TIN, registration number), requested when creating a new Vendor on the platform - a unique "SupplHi ID";
- Allowing a Vendor user to be associated with a specific "SupplHi ID". This association may be carried out by the registering Vendor User, by the Super User, or by a Buyer organization. An association made by a User to a Vendor where a Super User is already present must be confirmed by the Super User. The association gives the User the ability to view and manage information concerning their reference Vendor. The association is made under the sole responsibility of the person carrying it out and, where required, of the person providing the confirmation. SupplHi carries out no checks in this regard and cannot be held liable in the event of an incorrect association made by a User, Super User or Buyer organization. A Vendor User, as identified by a specific email address, may be associated with only one SupplHi ID and, therefore, with a single Vendor.
- Having one or more Vendor Super User(s) able to manage visibility and information management rights for Users connected to the same Vendor and to transfer or extend, on the platform and at any time, their Super User role to a specific colleague;
- Hosting on the platform the information provided by the Vendor during the various registration and completion stages, through dedicated Questionnaires, of the information requested by Buyer organizations, whether "industry-shared" or "customer-specific". It should be noted that the information entered by the Vendor on the platform in response to the Questionnaires may be of two types, clearly indicated on the platform within the individual Questionnaires:
    - "customer-specific": this information will only be visible to the specific Buyer organization clearly identifiable to the Vendor. Only that specific Buyer organization will be able to view, copy and use it.
    - "industry-shared": this information will potentially be visible to all Buyer organizations with access to the SupplHi platform. They will be able to view, copy and use it. The availability of "industry-shared" information reduces the effort required to fill in the typical information included in pre-qualification and qualification questionnaires (e.g. quality certifications held, number of employees, existence of a code of ethics, etc.) for multiple Buyer organizations, and increases visibility among the Buyer organizations using the platform.
- Supporting the Vendor in completing and updating the information requested by Buyer organizations within the Questionnaires, generating the list of missing information and carrying out - automatically or manually - "Quality Assurance" activity aimed at ensuring the consistency of the information provided by the Vendor with what was requested;
- Once the Vendor reaches 100% completion of the information and following the "Quality Assurance" activity, making the information provided by the Vendor visible - based on its type

("industry-shared" or "customer-specific") - to the Buyer organizations to which SupplHi grants access on the platform;

- Allowing the Vendor to expand its commercial channels for the sale of B2B supplies through the visibility gained with the Buyer organizations using the platform. We would like to point out that, by using our site, you allow all users of Buyer organizations to easily view and extract the "industry-shared" information you upload to our platform, using the tools we make available, and that such information may therefore circulate on the network even outside our control;
- Notifying the Vendor of information that is about to expire and allowing it to be updated on the platform;
- Allowing the Vendor to apply for Qualification processes with a specific Buyer organization;
- Allowing one or more Vendor ranking and scoring results to be viewed, based on the configuration carried out for the individual Buyer organization;
- Through the "Vendor Actions" functionality, allowing the Vendor to describe the corporate improvement actions it is implementing;
- Allowing the Vendor to receive RFx (requests for information, proposals, quotations) from Buyer organizations through the contacts provided by the Vendor;
- Through the "Management of Contractual Documents" module and the "Document Exchange" functionality, allowing the exchange of specific documents;
- Through the module called "SupplAuth", technically enabling access to other application systems configured by the Buyer organization (e.g. order management or tender systems). The authorization system is controlled exclusively by the Buyer organization, with SupplHi having no ability whatsoever to decide the authorization levels for the other applications;
- Supporting the Vendor through the publication of manuals and Frequently Asked Questions (FAQ) dedicated to Vendor users, and Help Desk activities through the ticketing system within the platform.

Any further Services and relationships between the Vendor and SupplHi are governed by the Terms and Conditions of the specific Service.

SupplHi undertakes to implement IT security measures appropriate to industry *standards* to protect all data and to provide the best possible service.

Cost of the service

SupplHi provides the Services described in this agreement to Vendors free of charge.

Account and User obligations

By using our site, you declare that you are not already subject to restrictions by SupplHi in the use of the Services and you undertake to:

1. activate only one personal account and ensure that your company has only one SupplHi account as a Vendor;
2. provide your real name and the real name of your company;
3. comply with all applicable legal provisions and internal policies such as, for example, personal data protection law, intellectual property law, anti-spam law, etc.;

4. use the Services offered by SupplHi only for professional and not personal purposes;
5. not act improperly by posting inappropriate or inaccurate content, not contact other users with any form of unwanted communication, and not engage in conduct that is unlawful or that is defamatory, offensive, obscene, discriminatory or otherwise objectionable;
6. not use or attempt to use the account of others;
7. not harm any other person or any other company using our site.

You undertake to choose a secure password, to keep it secret and not to share your account with anyone else. All users registering on the SupplHi platform are subject to a *password policy*.

To create your company's profile, you will answer the questions on the platform and, when necessary, update your answers. To this end, you guarantee that the information provided to SupplHi:

- is accurate;
- is promptly updated;
- does not contain anything that infringes the rights of third parties, that your company does not authorize you to share, or that is otherwise unlawful. By way of example, you undertake not to infringe the intellectual or industrial property rights of third parties, including patents, trademarks, trade secrets, copyrights or other rights, and not to add content that is not intended for, or accurate with respect to, the field to be completed (for example, entering a telephone number in the "email" field or in any other field);
- reflects the goods and services actually offered as a Vendor.

Information provided

When you provide us with information about your organization, others may view, copy and use such information. In particular, the information and content you provide us with will be viewed by users of Buyer organizations.

We inform you that, in order to provide our service to Vendors and Buyer organizations, and for *compliance* reasons, all interactions or changes to your profile as a Vendor on the platform are recorded and stored by SupplHi. For these reasons, you and SupplHi will be able to access such information. Only company data and no personal data - with the exception of the user's email - will be stored for this purpose.

In order to provide our service to Vendors and Buyer organizations, all interactions or changes to your Vendor's profile on the platform are recorded and made visible to Buyer organizations. Any personal data processed by SupplHi for this purpose will be handled in compliance with the data minimization principle set out in Article 25 of the GDPR and with all the security measures provided for in the Data Protection Agreement.

In order to provide users with a more complete service, the information you provide us with may be displayed together with other information that Buyer organizations using SupplHi may legitimately use in relation to your company and the services it provides (for example: financial soundness scores provided by financial rating agencies).

The information you upload to our site under either of the two methods - "industry-shared" and "customer-specific" as defined above - may be viewed and extracted by Buyer organizations according to the following rules.

- "customer-specific" information will not be accessible to other SupplHi Buyer organizations, and the exchange of information may also be subject to specific agreements - where in place - between your organization and the individual Buyer organization.
- SupplHi is built to prevent your competitors from viewing the "industry-shared" information you provide directly through our site. To this end, our platform is designed to manage visibility rights depending on the specific Buyer organization. Indeed, specific Buyer organizations have access to specific "industry-shared" information according to predetermined criteria and, in particular, based on the supply categories of the SupplHi Standard Categorization and the geographic areas of use. This controlled access is implemented to prevent Vendors and vertically integrated Buyer organizations from gaining access to information that would allow them to compare themselves with competitors on an individual basis. In the case of companies acting both as Buyer organizations and as Vendors, two separate profiles are provided, so that the Buyer organization's profile does not have access to information of companies active in the same supply families in which the Vendor is registered. Nevertheless, by using this service you agree that the information will be available on the Internet and, therefore, we would like to point out again that it will not remain secret.

None of the activities connected to third parties is imposed by SupplHi, which only provides the technical possibility of making the information available to Buyer organizations. For this reason, SupplHi cannot be held liable for damages, direct or indirect losses or other problems arising from the independent development of such relationships with third parties.

Management of information and of associations between Vendor and SupplHi ID

Each party is responsible for everything that happens in its own account. SupplHi will not modify the content of the information you provide us with, which will be published under your responsibility on our platform. However, we may modify the layout of the information if necessary to make it more readable to others.

When you view or use content and information provided by others published on our site, you do so at your own risk. SupplHi does not check the information provided by Buyer organizations or other parties and cannot guarantee its accuracy.

SupplHi is not liable for content or information provided by you, by other users or by third parties, nor for any damages arising from its publication, use, or reliance thereon by users or third parties.

By using our site, you also declare that you understand that the information you upload to SupplHi is not secret, but will be made available to SupplHi users in accordance with the rules specified above, and may also become generally known as a result of actions taken by third parties or Users for which SupplHi cannot be held responsible in any way. SupplHi is furthermore not in any way liable for any harmful consequence or damage that may result to you or third parties from the disclosure of such information.

The association of a Vendor user with a given "SupplHi ID", as described above, takes place under the sole responsibility of the person carrying it out and of the person providing the confirmation. SupplHi carries out no checks in this regard and cannot be held liable in the event of an incorrect association made by a User, Super User or Buyer organization.

If SupplHi is informed of the sharing of unlawful, incorrect or inappropriate information, it may be legally required to remove such information or content.

Rights to the information

The user retains ownership of the rights to the data uploaded and grants SupplHi an irrevocable, non-exclusive, worldwide license, including the rights of reproduction, processing, technical adaptation, storage, communication and any other use necessary for the operation, security, improvement and development of the platform. SupplHi reserves the right to use (e.g. analyze, process and publish), in aggregate form and also for commercial purposes, the non-personal "industry-shared" data made available by Users. In any case, personal data uploaded by users will not be used by SupplHi for any purpose other than the provision of the service.

Rights to the software

SupplHi reserves all intellectual and industrial property rights to the Services provided and the software made available, as well as to the information and databases generated through the use of the site or of the software.

By using our Service, you further undertake not to modify, copy or create derivative works of SupplHi, the Services or any related technology (except as expressly authorized by SupplHi), not to copy or use the information, content or data on SupplHi for system integration purposes or in connection with a competing service, not to decode, disassemble, decompile, decrypt or otherwise attempt to derive the source code for the Services or any related technology or part thereof, and not to monitor the Service, performance or functionality of SupplHi for any competitive purpose.

Use of the SupplHi logo

SupplHi authorizes your company to use the SupplHi logo and trademark in marketing materials (website, e-mails, brochures, presentations, etc.) solely for the purpose of identifying your company as a Vendor organization active on SupplHi. The logo may not be modified in any way and may only be used for the stated purpose. The logo must not be used in any way that could be considered derogatory or negative.

You also undertake not to use the word "SupplHi" in any trade name, email or URL without SupplHi's consent.

Artificial intelligence systems

SupplHi uses supervised artificial intelligence systems to carry out the "Quality Assurance" activity aimed at ensuring the consistency of the information provided by the Vendor with what is requested within the Questionnaires.

SupplHi allows users to use artificial intelligence systems for the purpose of:

- for Vendor Users, SupplHi and for the Buyer organizations - to carry out "Quality Assurance" of the information provided by the Vendors;
- for the Buyer organizations - to carry out "Vendor Scouting" activities.

The results generated by artificial intelligence are based on data and information that also includes data specifically made available by Vendor Users themselves while using the platform. SupplHi provides no warranty and assumes no liability, implied or explicit, with respect to the operation and the results obtained through the use of artificial intelligence tools.

Service improvements and changes

SupplHi may add, modify or delete any category of the Standard Categorization of goods and services, as well as any question addressed to the Vendor, in order to improve the service offered.

We may change or modify the prices of the service or some of these contractual terms. To the extent permitted by law, such changes will become effective unless the user exercises their right of withdrawal following appropriate notice from SupplHi.

Withdrawal

You may withdraw from this agreement at any time. Once you have withdrawn, you will lose the right to access or use the Service. Notwithstanding any such withdrawal, SupplHi users will retain the right to re-share content and information provided through the Service to the extent that it was copied or re-shared before the withdrawal.

If you wish to close your account, please contact our team at info@supplhi.com.

SupplHi reserves the right to suspend the use of its account if requested to do so by the competent authorities or in the event of a legitimate suspicion of unlawful use. If such unlawful use is confirmed, SupplHi reserves the right to terminate this agreement.

In the event of withdrawal, all personal data present is processed in accordance with the GDPR, as described in the Data Protection Agreement.

Applicable law and dispute resolution

In the unfortunate event of a dispute, the parties choose Milan (Italy) as the competent forum. Italian law applies.

How to contact us

Online at: www.supplhi.com

By email at: info@supplhi.com

[ENG] Data Processing Agreement - Designation as Data Processor for "Vendors"

SupplHi S.r.l. Società Unipersonale, with registered office at Via A. Calabiana, 6 - 20139 Milan (MI), Italy - Tax Code and VAT Number 09721660968 - Certified email (PEC): postmaster@pec.supplhi.com (hereinafter: the "Supplier");

and

the party accepting the Standard Terms and Conditions for the use of the SRM SaaS as a "Vendor" user (hereinafter: the "Customer"),

(hereinafter, collectively referred to as the "Parties").

Whereas:

a) the Customer - through the acceptance of the Standard Terms and Conditions for the use of the SRM SaaS by "Vendors" - has entered into an agreement with the Supplier (hereinafter: the "Agreement") for the provision, by the Supplier, of the SupplHi SRM SaaS service for Vendors (hereinafter: the "Services");

b) the performance of the aforementioned Services by the Supplier involves the processing, by the Supplier, on behalf of the Company, of personal data of data subjects for which the Company itself is the Data Controller (hereinafter: the "Personal Data"), as further specified in ANNEX 2: Scope of the Processing;

c) the Supplier declares that it has the experience, technical expertise and resources enabling it to implement adequate technical and organizational measures to ensure compliance with the regulations on the protection of personal data and the protection of data subjects;

d) by means of this Appointment Agreement, the Parties intend to govern the processing and protection of Personal Data in accordance with applicable laws and regulations, including Regulation (EU) 2016/679 of 27 April 2016, on the protection of natural persons with regard to the processing of personal data - the General Data Protection Regulation (hereinafter: the "GDPR" or the "Regulation");

e) the Customer and the Supplier are also referred to below, respectively, as the Data Controller and the Data Processor;

f) for the purposes of this Appointment Agreement, the terms "Data Controller", "Data Processor", "data subject", "processing", and "Supervisory Authority" shall have the respective meanings attributed to them by the GDPR.

Now, therefore (with the foregoing recitals forming an integral and substantive part of this Data Processing Appointment Agreement), the Parties hereby agree and stipulate as follows

1. Purpose

1.1 The Parties expressly acknowledge and accept that, with respect to the processing of Personal Data, the Company acts as the Data Controller. As such, it is solely responsible for the accuracy and lawfulness of the Personal Data, for its use under the Agreement, and for the lawfulness of the means by which it was obtained.

1.2 The Company appoints the Supplier, pursuant to Article 28 of the GDPR, as Data Processor for the processing of Personal Data connected with the provision of the Services.

2. Scope of the Processing

2.1 The purpose of the processing of Personal Data by the Supplier is the performance of the Services under the Agreement. The nature of the processing, the type of Personal Data processed and the categories of data subjects are further specified in ANNEX 2: Scope of the Processing.

3. General obligations of the Processor

3.1 Personal Data shall be processed by the Processor in accordance with the applicable rules on the processing of personal data, with this appointment instrument, and with any reasonable instructions received in writing from the Company, provided that such instructions are consistent with the terms of this appointment instrument, and solely and exclusively to the extent strictly necessary for the performance of the Services under the Agreement, with any other and different use being expressly excluded.

3.2 The only possible exception to the provisions of paragraph 3.1 above is the existence of a legal obligation or a reasoned request from an administrative or judicial Authority, including Supervisory Authorities (hereinafter: the "Authorities"), in which case the Processor, to the extent permitted by law or by the orders of the Authority, shall inform the Company of any processing of Personal Data that differs from or exceeds that provided for in this appointment instrument.

3.3 The Processor undertakes to establish and keep up to date the register of processing activities carried out by the Processor on behalf of the Company.

4. Security obligations

4.1 The Processor, taking into account the risks arising from the destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, whether accidental or unlawful, shall adopt and maintain adequate technical and organizational measures to protect the security, confidentiality and integrity of the Personal Data, taking into account, among other things, the type of processing, the purposes pursued, the context and the specific circumstances in which the processing takes place, as well as the applicable technology and the costs of implementation.

4.2 The Processor undertakes to adopt the physical, logical and organizational security measures provided for by ISO 27018. Such measures may only be changed provided that a level of security at least equal to that existing at the time this appointment instrument is signed is maintained.

4.3 Any developments and/or changes to the security measures requested by the Controller shall be subject to a specific cost quotation by the Supplier and must be approved in writing by both parties.

4.4 The Processor further undertakes to provide the Company with cooperation in relation to the Controller's obligation to implement adequate technical and organizational measures, pursuant to Article 32 of the GDPR.

5. Persons authorized to process

5.1 Without prejudice to the provisions of Article 12 below, the Processor guarantees that access to Personal Data will be limited to its own employees and collaborators, to the extent necessary for the performance of the Services and provided that they have been appropriately instructed, pursuant to paragraph 5.2 below, regarding the methods of processing Personal Data and the technical and organizational security measures in place to protect Personal Data.

5.2 The Processor undertakes to designate in writing its employees and collaborators responsible for processing Personal Data owned by the Company, by means of specific letters of appointment, identifying the scope of processing permitted and providing them with appropriate instructions for this purpose, in particular binding them to confidentiality regarding all information acquired in the course of their activity, including for the period following the termination of the employment relationship.

6. Personal Data Breaches (the "*Data Breach*")

6.1 The Supplier undertakes to notify the Company, in writing and without undue delay, of any Personal Data Breach suffered by it or notified to it by any Sub-processor. In particular, the Supplier undertakes to inform the Controller of any security breach that accidentally or unlawfully results in the destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed, and to provide the Controller with all necessary cooperation in connection with the fulfilment of its obligations to notify such breaches to the Authority pursuant to Article 33 of the GDPR or to communicate them to data subjects pursuant to Article 34 of the GDPR.

6.2 The Controller shall have the right to carry out any verification, including at the Processor's premises, useful for verifying the Processor's compliance with the provisions of this article, including through the completion of self *assessment* questionnaires.

7. Impact assessment (the "Data Protection Impact Assessment")

7.1 The Processor undertakes to provide the Controller with any information useful for the Controller to carry out the data protection impact assessment, should the Controller be required to carry it out pursuant to Article 35 of the Regulation, as well as any cooperation in carrying out any prior consultation with the Supervisory Authority pursuant to Article 36 of the Regulation.

8. System Administrators

8.1 The Data Processor shall comply with applicable data protection laws, including the GDPR, and all relevant guidelines issued by the Supervisory Authority regarding the role and duties of system administrators.

8.2 The Supplier undertakes, in particular, to:

i) designate as system administrators the professional figures dedicated to the management and maintenance of processing systems or components thereof with which Personal Data is processed;

ii) prepare and keep an up-to-date list containing the identifying details of the natural persons designated as system administrators and the functions assigned to them.

9. Relations with the Authorities

9.1 The Processor, at the Controller's request, undertakes to assist the latter in the event of proceedings before the supervisory authority or judicial authority, including by allowing the Controller to promptly produce privacy documentation and supporting documents falling within the Processor's competence.

10. Requests from Data Subjects

10.1 If a data subject contacts the Processor directly to exercise their rights, the Processor must handle the request and respond to the data subject within one month. If this is not possible, the Processor, to the extent permitted by law, shall notify the Controller of the request.

10.2 Taking into account the nature of the processing, the Processor shall assist the Company, to the extent possible, with appropriate technical and organizational measures, in fulfilling the Company's obligation to respond to data subjects' requests pursuant to the applicable rules in this regard.

11. Reporting and Audits

11.1 The Processor shall make available to the Controller all the information necessary to demonstrate compliance with the obligations set out in the aforementioned regulations and/or the Controller's instructions under this appointment instrument, and shall allow the Data Controller to exercise its powers of control and inspection, providing all reasonable cooperation for the *audit* activities carried out by the Controller, for the purpose of verifying compliance with the obligations and instructions set out in this appointment instrument. It is understood that any verification conducted pursuant to this article must be carried out in such a way as not to interfere with the normal course of the Processor's business and providing the Processor with reasonable advance notice.

12. Sub-processors

12.1 The Supplier may engage further processors to process Personal Data owned by the Company (hereinafter: the "Sub-processors"). This agreement constitutes the general authorization referred to in Article 28(2) of the GDPR to use the Sub-processors currently engaged by the Supplier. The list of current Sub-processors is set out in ANNEX 3 - List of Sub-processors.

12.2 The Processor undertakes to impose on its Sub-processors in writing, through specific binding agreements, the same obligations regarding the protection of Personal Data to which the Processor is subject under this appointment instrument, particularly with regard to security obligations.

12.3 The Processor expressly undertakes to inform the Company of any changes concerning the addition or replacement of further Sub-processors. The Company shall have the right to object to such changes by notifying its objection in writing within 3 calendar days of notification by the Processor. In the absence of an objection, the change shall be deemed accepted.

12.4 It is expressly understood that the Processor shall remain directly liable to the Company for the acts and omissions of its Sub-processors.

13. Return and deletion of personal data

13.1 Upon expiry of the Agreement and/or termination of the Services, or in any case in the event of termination of the effectiveness of this appointment instrument for any reason, unless there is a legal or national/EU regulatory obligation requiring the retention of Personal Data, the Processor shall cease all processing operations and shall immediately return the Personal Data to the Controller.

14. Term

14.1 This appointment shall take effect from the date on which it is signed by the Parties and shall remain valid until termination of the Agreement and/or the Services for any reason, or until early revocation for any reason by the Controller.

15. Data Protection Officer (the "DPO")

15.1 The Data Protection Officer designated by the Data Processor, pursuant to Article 37 of the GDPR, is Francesco Garrassino (privacy@supplhi.com).

ANNEX 1 - Technical and Organizational Measures

In addition to the security measures set out in the Agreement and the DPA, the Data Processor shall apply the following organizational security measures.

Confidentiality, integrity, availability and resilience of systems

Infrastructure. SupplHi servers hosted in the cloud at Amazon Web Services data centers in the European region (currently "eu-west-1", Ireland), in compliance with the data residency requirements set out by the GDPR.

Access control. Role-based access management (RBAC), based on the principle of least privilege.

Authentication. Multi-factor authentication (MFA) mandatory for "Vendor" users' access to the platform. "Buyer" Customers may integrate their own Single Sign-On, both for authentication (SAML) and for de/provisioning (SCIM).

Environment segregation. Logical separation between development, test and production environments.

Data segregation. Logical isolation of data in a multi-tenant architecture: each record is associated with a specific tenant and accessible, through application authorization and filtering mechanisms, only to users of the same tenant; the effectiveness of the isolation controls is verified as part of testing and application security processes.

Logging and monitoring. Continuous recording and monitoring of access and system activities.

Perimeter protections. Firewalls and intrusion detection systems, including the use of a WAF (Web Application Firewall).

Vulnerability management. Structured vulnerability management process and regular system patching.

Encryption and pseudonymization

Data in transit. Encryption via TLS 1.2 or higher protocol for all client-server communications and between internal services.

Data at rest. Encryption of databases and storage using the native tools of the AWS cloud provider.

Key management. Management of encryption keys via a dedicated service of the AWS cloud provider.

Ability to restore the availability of and access to data

Backup. Backups performed on a daily basis, with monitoring of the outcome and a retention period of 18 months.

Restore testing. Quarterly verification of backup integrity through restore tests.

Disaster Recovery. Disaster Recovery and Business Continuity Plan with an RPO (Recovery Point Objective) target of 36 hours and an RTO (Recovery Time Objective) target of 48 hours.

Redundancy. Infrastructure redundancy across multiple Availability Zones in the AWS eu-west-1 region (Ireland) – physically separate data centers within the same region – to ensure high availability and resilience in the event of a disaster; the ability to relocate the entire infrastructure to another European AWS region (e.g., eu-central-1, Frankfurt), while maintaining data residency within the EU, is verified as part of periodic Disaster Recovery tests.

Periodic testing and verification of the effectiveness of the measures

Certifications. ISO/IEC 27001:2022 certification issued by Bureau Veritas for the "Management of a SaaS platform for the collection and management of Vendor Management information", in accordance with the Statement of Applicability, supplemented by the controls of the ISO/IEC 27017:2015 and ISO/IEC 27018:2019 guidelines. Availability of SOC 1 Type II reports (EY audit) on general IT controls relevant to Customers' financial reporting, covering the change management, access, operations and infrastructure processes that feed, through application integrations, Customers' ERP/management systems.

Penetration testing. Vulnerability assessment and penetration testing (VA/PT) performed at least annually and following significant releases, carried out by a leading Cyber Security firm, with subsequent management and remediation of any vulnerabilities identified.

Incident management. A specific procedure aimed at managing events and incidents with a potential impact on personal data, defining roles and responsibilities, the detection process (suspected or confirmed), the implementation of countermeasures, the response to and containment of the incident/breach, as well as the procedures for notifying the Customer of personal data breaches.

Organizational measures

Security policies. Information Security Management System (ISMS) compliant with ISO 27001, ISO 27017 and ISO 27018, with internal policies documented and maintained through update cycles.

Training. Periodic staff training on data protection and information security.

Staff confidentiality. Non-disclosure agreements (NDAs) signed by employees and contractors with access to data.

Sub-processor management. Due diligence and qualification of sub-processors, with contractual imposition of equivalent obligations through cascading data processing agreements.

Data retention. Data retention policies and secure data deletion procedures upon termination of the contractual relationship or upon request of the Controller.

Privacy by design. "Privacy by design and by default" approach in the development of new platform features.

Physical security

Physical security. Delegated to the AWS cloud provider, certified 27001/27017/27018 (cloud security and privacy), SOC 1, 2 and 3 for its data centers, which include physical access controls, video surveillance, redundant power supply and fire protection.

ANNEX 2 - Scope of the Processing

This annex forms an integral part of the Data Processor Appointment Agreement.

Categories of data subjects: supplier users who register on the SupplHi platform and their colleagues referenced in questionnaire responses.

Type of Personal Data processed. The Personal Data processed are exclusively those indicated below:

- First name, last name and company email address.
- Non-application log files (for example: platform access, the trace of requests made to the back-end, etc.) generated by supplier users while using the SupplHi platform.
- In the case of supplier users defined as “Individuals”, tax data and IBAN or other bank account-related data.
- In some cases, a company telephone number may also be required.

Nature and purpose of processing: access to SaaS on the SupplHi platform.

Duration of processing: until the purposes are achieved and in accordance with the retention terms provided by law.

ANNEX 3 - List of Sub-processors

The following Sub-processors are used by SupplHi:

Name	*Billing address*	*Description of the processing*	*Certification*	*Location of the processing*
Amazon Web Services EMEA SARL	38 avenue John F. Kennedy L-1855 Luxembourg	• Hosting • Data storage • Backup	• ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019 • ISO/IEC 27701:2019 • ISO/IEC 22301:2019 • ISO/IEC 9001:2015	Europe
Microsoft S.r.l.	Microsoft House Viale Pasubio 21 20154 Milan (MI), Italy	• Azure Active Directory • OneDrive	• ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019	Europe
Google Cloud Italy S.r.l.	Via Federico Confalonieri 4 20124 Milan, Italy	• Google Cloud • Gemini	• ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019	Europe
Aruba S.P.A.	Via S. Clemente, 53 - 24036 Ponte San Pietro (Bergamo), Italy	• Email management	• ISO/IEC 27001:2022 • ISO/IEC 27017:2015 • ISO/IEC 27018:2019	Europe
Atlassian Pty Ltd	Level 6, 341 George St, - Sydney NSW 2000, Australia	• Internal Ticket Management	• ISO/IEC 27001:2022 • ISO/IEC 27018:2019	Europe