Agreement on Processing of Personal Data (Data Processing Agreement)

hellotax Global S.L. – Annex to the hellotax Terms & Conditions – Last updated: 30/10/2026

concluded between the following parties (hereinafter referred to as the "Agreement"):

(1)**HELLOTAX GLOBAL, S.L.**
Comp. Reg. No.: B54751110,
Tax Id. No.: ESB54751110
with the registered office at: Calle Versalles, 3C, CP 03560, El Campello, Alicante, Spain
registered in the Commercial Register of Alicante, Volume (Tomo) 3741, Folio 157, Sheet (Hoja) A-138003.
represented by: Cristian Noguera de Erquiaga

(hereinafter referred to as the "**Processor**" or "**hellotax**")

and

(2)the Customer, being the legal entity or entrepreneur that has contracted the hellotax services, as identified in its subscription and customer account under the hellotax Terms & Conditions,
represented by its authorised representative

(hereinafter referred to as the "**Controller**" or the "**Customer**")

(The Controller and the Processor hereinafter referred to collectively as the "**Parties**")

Preamble

Whereas:

(a)The Controller and the Processor entered into the hellotax Terms & Conditions, including the Software-as-a-Service Agreement, the Fiscal Services Agreement and their schedules (hereinafter referred to as the "**Principal Agreement**"), accepted by the Customer upon subscription to the hellotax services;

(b)Regarding the performance of the Principal Agreement, personal data shall be processed and transferred between the Parties, with the Parties being interested in laying down the rights and obligations in relation to the transfer and processing of personal data provided between the Parties in order to comply with all the legal obligations, particularly arising out of the regulation (EU) 2016/679 of the European Parliament and of the Council 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 (General Data Protection Regulation) (hereinafter referred to as the "**GDPR**") and Spanish Organic Law 3/2018 of 5 December on the Protection of Personal Data and Guarantee of Digital Rights (hereinafter referred to as the "**LOPDGDD**"),

the Parties have agreed as follows:

Article 1 – Introductory Provisions

1.1. This Agreement is entered into in order to process and ensure the protection of personal data processed by the Processor as part of the performance of the Principal Agreement, namely the VAT compliance services provided by the Processor to the Controller, including VAT registration, VAT calculation, the preparation and submission of VAT returns and related filings, and the related communications with tax authorities (hereinafter referred to as the "**Service**").

1.2. This Agreement forms an integral part of the Principal Agreement and is concluded upon the Controller's acceptance of the hellotax Terms & Conditions. A separate signature by the Parties is not required for its validity.

1.3. Roles of the Parties. With respect to the personal data of the Controller's own customers or buyers (B2C and B2B) (hereinafter referred to as the "**End Users**") processed in the provision of the Service, the Customer acts as controller and hellotax acts as processor. With respect to personal data processed in the direct contractual relationship between hellotax and the Customer (contract management, billing and payment collection, customer support, call recordings and marketing communications), hellotax acts as an independent controller; such processing is governed by the hellotax Privacy Policy and is not subject to this Agreement.

Article 2 – Authorization and scope of Processed Data

2.1. Authorization of the Processor. Within the meaning of Article 28 of the GDPR, the Controller hereby authorizes the Processor to process personal data, to which the Processor shall obtain access while providing the Service, to the extent and under the terms and conditions set out herein and the Processor accepts this commitment and undertakes to perform it properly. The Processor is obliged to process personal data in accordance with the Agreement, generally binding regulations, including without limitation to, the GDPR and the LOPDGDD.

2.2. Scope and Purpose of Processing. Personal data shall be processed solely for the purpose of performing the Service and only to the extent necessary for its provision. The subject matter, duration, nature and purpose of the processing, the types of personal data and the categories of data subjects are described in Appendix 1.

2.3. Method of Processing. Personal data shall be transferred between the Parties primarily electronically in the form of digitized data, including through the retrieval of transaction data by the Processor from the sales platforms used by the Controller (such as Amazon and Shopify) via API connections authorised by the Controller. If it is necessary or appropriate, the Parties may also agree that, in a specific case, personal data shall be transferred in paper form. If it complies with the obligations under the Principal Agreement, the Processor shall temporarily store the provided personal data on a data carrier and, for the time necessary for the processing of personal data, it shall use and keep them in order to fulfill the obligations under the Principal Agreement. In this context, the Processor undertakes to ensure the technical and organizational measures for securing personal data protection. Each of the Parties shall fulfill its obligations under the generally binding regulations, including the exercise of the rights of the data subjects and the fulfillment of the information obligation in accordance with the relevant provisions of the generally binding regulations.

2.4. Period. The Processor shall process personal data for as long as it is necessary for the fulfillment of the purposes of this Agreement and the Principal Agreement, not longer than until the termination of this Agreement, unless otherwise stipulated by the generally binding regulations or unless otherwise agreed by the Parties.

2.5. Controller's Instructions. The Processor declares and undertakes to process personal data only on the basis of documented instructions from the Controller, including with regard to transfers of personal data to a third country or an international organisation, unless required to do so by Union or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest. Similarly, this applies to the Processor's statutory body and the Processor's employees who have access to the processed personal data in the course of their work. The Principal Agreement and the Controller's use of the functionalities of the Service constitute the Controller's documented instructions. Any additional instructions shall be given electronically to the e-mail address indicated in Article 8 or in writing to the address of the Processor's registered office. The Processor is obliged to immediately inform the Controller if, in its opinion, an instruction infringes the GDPR or other Union or Member State data protection provisions. If the Controller insists on the infringing instruction even after the Processor's notice, the Processor may unilaterally withdraw from this Agreement.

2.6. Processing beyond the Scope of the Agreement. Article 28(10) GDPR shall apply where the Processor determines the purposes and means of processing in breach of this Agreement.

2.7. Place of Processing and International Data Transfers.

(a)The Processor shall primarily process personal data within the European Economic Area (EEA).

(b) The Processor may transfer personal data to, or engage sub-processors located in, countries outside the EEA, provided that such transfers comply with Chapter V GDPR, in particular where: (i) the European Commission has adopted an adequacy decision pursuant to Article 45 GDPR in respect of the relevant country or framework, including the United Kingdom and, for certified organisations, the EU-U.S. Data Privacy Framework; or (ii) appropriate safeguards pursuant to Article 46 GDPR are in place, such as the Standard Contractual Clauses adopted by the European Commission, together with supplementary measures where required including remote access to personal data by personnel of sub-processors located outside the EEA.

(c) Where the Controller instructs the Processor to provide VAT registration, filing or representation services in a country outside the EEA, the transfer of the personal data necessary for such services to the competent tax authorities and to local tax agents or fiscal representatives engaged for that purpose shall be deemed to be carried out on the documented instructions of the Controller. The Processor shall ensure that such transfers to its agents or representatives are subject to an appropriate transfer mechanism under Chapter V GDPR.

(d) The Processor shall make available to the Controller, upon request, information on the locations of processing and the transfer mechanisms relied upon, as reflected in the list of sub-processors referred to in Article 3.

Article 3 – Sub-processors of the Processor

3.1. General Authorisation. The Controller grants the Processor a general written authorisation pursuant to Article 28(2) GDPR to engage sub-processors. The current list of sub-processors, including their location and the transfer mechanism relied upon, is set out in Appendix 2 and is published inside the Hellotax platform . It is deemed approved by the Controller upon acceptance of the hellotax Terms & Conditions.

3.2. Changes and Objections. The Processor shall inform the Controller of any intended addition or replacement of sub-processors at least 14 days in advance, by updating the list referred to in Article 3.1 and by e-mail notification to Customers who have subscribed to such notifications. The Controller may object to such change on reasonable data protection grounds by written notice within this period. The Parties shall discuss the objection in good faith; if no solution is reached, the Controller may terminate the affected Services with effect from the date on which the new sub-processor is engaged, as its sole remedy.

3.3. The Processor is obliged to impose on its sub-processors, by way of a contract or other legal act under Union or Member State law, the same personal data protection obligations as set out in this Agreement between the Controller and the Processor, including, without limitation to, providing sufficient guarantees as to the introduction of appropriate technical and organizational measures in order the processing complies with the requirements of the LOPDGDD and the GDPR.

3.4. The Processor acknowledges that if a particular sub-processor fails to fulfill its data protection obligations, it shall be fully liable for the fulfillment of the obligations of that sub-processor to the Controller, in accordance with Article 28(4) GDPR.

3.5. Independent tax accountants. The tax assistance services under the Fiscal Services Agreement (“hellotax Accountants”) are performed by independent tax accountants engaged by the Processor under written service agreements. Such accountants act as sub-processors of the Processor and are subject to this Article 3.

Article 4 – Technical and Organizational Security of Personal Data Protection

4.1. The Processor undertakes to implement technical and organizational protection of the processed personal data in accordance with Article 32 GDPR in order to prevent unauthorized or accidental access to the personal data, their modification, destruction or loss, unauthorized transfers, any other unauthorized processing as well as other misuse, and throughout the processing of the data, that all obligations regarding processing of the personal data resulting from the generally binding regulations and ISO

standards – if they are applicable – are continuously secured in terms of personnel and organizational measures.

4.2. The Processor hereby declares that the personal data protection is subject to the Processor's internal security guidelines within its information security management system. The Processor undertakes to periodically review the technical and organizational measures for the personal data protection, to evaluate their effectiveness and to update them taking into account the state-of-the-art technologies and the probability and seriousness of risks in the security of the processing of personal data.

4.3. The Processor undertakes to secure the processing of personal data in the following ways, including without limitation to:

(i) access to personal data shall only be granted to Processor's authorized persons who shall agree with the Processor on the conditions and extent of the processing of data and any such person shall access personal data under his/her unique identifier;

(ii) Processor's authorized persons who process personal data hereunder are required to maintain confidentiality of personal data and security measures whose disclosure would jeopardize their security. The Processor shall ensure their demonstrable commitment to this obligation. The Processor shall ensure that this obligation for the Processor as well as the authorized persons will continue even after the termination of their employment or other relationship with the Processor.

4.4. The technical and organisational measures implemented by the Processor are described in Appendix 3. The Processor may update them from time to time, provided that the overall level of security is not reduced.

Article 5 – Reporting Security Incidents

5.1. Once the Processor becomes aware that a personal data breach has occurred, it is required to notify the Controller of such a breach without undue delay, but no later than within 48 hours after having become aware of it, unless such a breach is unlikely to result in a risk to the rights and freedoms of natural persons.

5.2. If the Controller is not notified within 48 hours at the latest, the Processor must state the reasons for the delay at the same time.

5.3. The notification must include particularly:

(i) a description of the nature of the personal data breach, including, where possible, the categories and approximate number of data subjects concerned and the approximate number of personal data records concerned;

(ii) a description of the likely consequences of the personal data breach;

(iii) a description of the measures taken or proposed to be taken by the Processor to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects; and

(iv) the name and contact details of the Processor's contact point where more information can be obtained.

5.4. Where, and in so far as, it is not possible to provide all the information at the same time, the information may be provided in phases without undue further delay. The Processor shall assist the Controller in fulfilling its obligations under Articles 33 and 34 GDPR, taking into account the nature of processing and the information available to the Processor.

Article 6 – Termination of the Processing

6.1. This Agreement is concluded for the term of the Principal Agreement. Termination of the Principal Agreement for any reason results in the automatic termination of this Agreement on the date on which the Principal Agreement is terminated unless otherwise agreed by the Parties in writing.

6.2. This Agreement may also be terminated by written agreement of the Parties.

6.3. The Controller is entitled to withdraw unilaterally from this Agreement in the event of serious violation of any of the Processor's obligations arising from this Agreement or generally binding regulations. Serious violation of this Agreement is, including without limitation to, violation of the Processor's obligations referred to in Articles 3, 4, 5, 6 and 7 hereof.

6.4. Personal data shall be processed and stored by the Processor for the term of the Principal Agreement.

6.5. Upon termination of the Principal Agreement, the Processor shall be obliged to return the retained personal data to the Controller, upon the Controller's written request, on a suitable data medium or in electronic downloadable form within 30 calendar days of the termination of the Principal Agreement or of the Controller's request, whichever is later.

6.6. Upon the transfer of personal data back to the Controller, or where the Controller has not requested their return, the Processor undertakes to destroy the not transferred personal data, e.g. to erase them from the electronic storage system or to shred documents, without delay but no later than within three calendar months after termination of the Principal Agreement, unless Union or Member State law requires storage of the personal data, in particular statutory retention obligations applicable to tax records; in such case the Processor shall restrict the processing of such data to compliance with that obligation.

Article 7 – Confidentiality

7.1. The Processor declares and undertakes to treat all data related to the Service as confidential, undertakes to maintain confidentiality of them, i.e. it shall not disclose them to anyone except its employees and particular sub-processors and only to the extent necessary for the provision of services, or where disclosure is required by law, in particular to competent tax authorities in the performance of the Service. This obligation of confidentiality persists even after the termination of this Agreement.

Article 8 – Miscellaneous Provisions

8.1. Information and audits. The Processor shall make available to the Controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 GDPR and shall allow for and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. Audits shall be carried out with at least 30 days' prior written notice, during normal business hours, no more than once per calendar year (except following a personal data breach or at the request of a supervisory authority), at the Controller's cost and without undue disruption to the Processor's operations; the auditor shall be bound by confidentiality. The Processor may first satisfy an audit request by providing relevant documentation, certifications or audit reports.

8.2. Cooperation and data subject rights. The Parties undertake, if necessary, to provide, without undue delay, full cooperation in dealing with and negotiating with the competent supervisory authority, in particular the Spanish Data Protection Agency (Agencia Española de Protección de Datos) and with the data subjects concerned by the processing of personal data, including without limitation to, in exercising their rights of access to their data, the right to rectify or erase them. Taking into account the nature of the processing, the Processor shall assist the Controller by appropriate technical and organisational measures, insofar as possible, in fulfilling its obligation to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR. The Processor shall promptly forward to the Controller any such request received directly from a data subject and shall not respond to it without the Controller's instruction.

8.3. Impact assessments and prior consultation. The Processor shall assist the Controller in ensuring compliance with the obligations pursuant to Articles 32 to 36 GDPR, including data protection impact assessments and prior consultations with the supervisory authority, taking into account the nature of processing and the information available to the Processor.

8.4. Contact points. The Processor's contact point for data protection matters is: hellotax Global S.L., Calle Versalles, 3C, CP 03560, El Campello, Alicante, Spain; e-mail: legal@hellotax.com.

The Controller's contact point is the contact person and e-mail address designated in its hellotax customer account.

Each of the Parties may unilaterally change its contact person by delivering a written notice of the change of the contact person to the other Party.

8.5. Liability. Each Party's liability under this Agreement shall be subject to the limitations of liability set out in the Principal Agreement, without prejudice to the rights of data subjects under Article 82 GDPR.

8.6. Order of precedence. In the event of any conflict between this Agreement and the Principal Agreement, this Agreement shall prevail with respect to the processing of personal data on behalf of the Controller.

Article 9 – Final Provisions

9.1. This Agreement shall enter into force and effect on the date on which the Controller accepts the hellotax Terms & Conditions.

9.2. This Agreement may be supplemented or amended only in writing or in accordance with the procedure for changes set out in the hellotax Terms & Conditions. Changes to Appendix 2 shall follow the procedure set out in Article 3.

9.3. In the event that any provision of this Agreement is or becomes invalid or ineffective, this shall not affect the other provisions of this Agreement, and the Parties undertake to replace such invalid or ineffective provision of this Agreement with another, valid and effective provision which by its very best purpose corresponds to the purpose of this Agreement, within 30 (thirty) calendar days of the date on which the last Party has been notified of the invalidity or ineffectiveness of such an arrangement.

9.4. None of the Parties may assign the Agreement, a single commitment from the Agreement or claims arising in connection with this Agreement to other persons without the prior written consent of the other Party, save that the Processor may assign this Agreement together with the Principal Agreement to an affiliate or to a successor in the context of a merger, acquisition or transfer of all or substantially all of its business.

9.5. This Agreement shall be governed by the laws of Spain. The courts of Alicante shall have jurisdiction, without prejudice to the powers of the competent supervisory authorities.

9.6. The Parties declare that they have read this Agreement, that it has not been concluded under obviously disadvantageous conditions, and that it is accepted by the Controller together with the hellotax Terms & Conditions.

Appendix 1 – Description of the Processing

Item	Description
Subject matter	Processing of the Controller's sales transaction data, including personal data of End Users, for the provision of VAT compliance services.
Duration	The term of the Principal Agreement, plus the period for return and deletion set out in Article 6 and any statutory retention period applicable to tax records.
Nature of the processing	Collection (via authorised API connections to sales platforms or upload by the Controller), recording, structuring, storage, calculation, consultation, transmission to tax authorities and tax agents, retention and erasure.
Purpose	VAT calculation; VAT registration; preparation and submission of VAT returns, recapitulative statements and other tax filings; communications with tax authorities; Tax Letter Inbox.
Categories of data subjects	End Users of the Controller (B2C and B2B buyers) and, for B2B buyers, their contact persons.
Types of personal data	Name; billing and delivery address; country of residence or delivery; e-mail address and telephone number where included in transaction data; VAT identification number or other tax ID; order and invoice numbers; transaction dates, amounts and currency; goods or services purchased; payment method type (no payment card data).
Special categories of data	None.

Appendix 2 – List of Sub-processors

The current list of sub-processors is published inside the Hellotax platform. As at the date of this Agreement, it comprises:

Sub-processor	Purpose	Location	Transfer safeguard
Scaleway SAS	Hosting and cloud infrastructure	France	EU/EEA – no transfer
Google Ireland Ltd (Google Workspace)	E-mail, file storage and document collaboration	EU / USA	EU-U.S. DPF; SCCs
Atlassian (Jira)	Service operations and task management	USA / Australia	EU-U.S. DPF; SCCs
Zendesk	Customer support	USA	EU-U.S. DPF; SCCs
Dropscan GmbH	Scanning of postal correspondence from tax authorities	Germany	EU/EEA – no transfer
Alohi SA (Fax.plus)	Fax communications with tax authorities	Switzerland	Adequacy decision
CEGID	Accounting software for French VAT filings	France	EU/EEA – no transfer
Zapier	Workflow automation	USA	EU-U.S. DPF; SCCs
Twilio Inc. (SendGrid)	Transactional e-mail delivery	USA	EU-U.S. DPF; SCCs
VAT Digital Limited	VAT registration, filing and fiscal representation (IT, IE, BE, UK, NL)	United Kingdom	Adequacy decision
Verico Paris SAS	VAT registration, filing and fiscal representation (FR)	France	EU/EEA – no transfer
Independent tax accountants	Preparation and submission of VAT returns	EU/EEA	EU/EEA – no transfer
Room 714 SLU	Software development and maintenance	Spain	EU/EEA – no transfer

DPF: EU-U.S. Data Privacy Framework. SCCs: Standard Contractual Clauses adopted by the European Commission.

Appendix 3 – Technical and Organisational Measures

1. Scope

This Appendix describes the technical and organisational measures implemented by hellotax Global S.L. ("hellotax") pursuant to Article 32 GDPR to ensure a level of security appropriate to the risk when processing personal data on behalf of its Customers under the Agreement. The measures take into account the state of the art, the costs of implementation and the nature, scope, context and purposes of the processing, as well as the risks for the rights and freedoms of natural persons.

The measures apply to the hellotax application (app.hellotax.com), its supporting infrastructure, and the business tools, personnel and contractors involved in the provision of the Service. Measures implemented by sub-processors are governed by their respective data processing agreements in accordance with Article 3 of the Agreement.

2. Governance and policies

- **Responsibility:** a designated person within hellotax is responsible for data protection and information security matters and can be contacted at legal@hellotax.com.
- **Policies:** hellotax maintains internal guidelines on information security, acceptable use of systems, data handling and incident response, which are binding on all personnel and contractors.
- **Records:** hellotax maintains a record of processing activities carried out as processor in accordance with Article 30(2) GDPR.
- **Review:** the measures described in this Appendix are reviewed at least once a year and whenever there is a significant change to the Service or its infrastructure.

3. Personnel and contractors

- **Confidentiality:** all employees and contractors with access to personal data are bound by written confidentiality obligations that survive the end of their engagement.
- **Contractual safeguards:** contractors processing personal data are engaged under written data processing agreements pursuant to Article 28(4) GDPR. Contractors located outside the EEA are additionally bound by the Standard Contractual Clauses adopted by the European Commission, supported by a documented transfer impact assessment.
- **Training:** personnel and contractors receive data protection and information security training upon onboarding and periodically thereafter at least annually.
- **Need-to-know:** personnel and contractors only receive access to the personal data required for their specific tasks.
- **Offboarding:** access rights are revoked without undue delay, and in any case within 24 hours, upon termination of employment or engagement, and company equipment and data are returned or securely erased.

4. Access control

- **Unique accounts:** each user accesses systems with an individual account; shared accounts are not used for systems processing personal data.
- **Least privilege:** access rights are role-based and limited to what is necessary for each role. Administrative and production access is restricted to a limited number of authorised technical staff.
- **Multi-factor authentication:** multi-factor authentication is enforced for administrative and production access and for Zendesk, Google Workspace, Jira and other applications where available. hellotax is extending mandatory multi-factor authentication to all business applications processing customer data.
- **Passwords:** passwords must meet minimum complexity requirements and are managed through single sign-on.

- **Access reviews:** access rights to systems processing customer data are reviewed periodically at least every six months.
- **Sessions:** user sessions in the hellotax application expire after a period of inactivity, and devices lock automatically when unattended.

5. Data handling and minimisation

- **Data collection:** transaction data is retrieved from sales platforms only through API connections authorised by the Customer and limited to the data necessary for VAT compliance purposes.
- **Purpose limitation:** customer data is used exclusively to provide the Service; no profiling, marketing or other secondary use is made of End User data.
- **Working within systems:** personal data is processed primarily within the hellotax application and approved business tools. Downloading files containing personal data (for example, transaction reports or VAT return documents) is permitted only where strictly necessary for the performance of a specific task, onto encrypted devices, and such files must be deleted once the task has been completed.
- **Prohibited storage:** storing customer data on personal cloud services, removable media or unapproved devices is prohibited.
- **Transmission to authorities:** VAT returns and related documents are transmitted to tax authorities through the official electronic channels provided by those authorities, or through engaged tax agents.

6. Encryption

- **In transit:** all connections to the hellotax application and its APIs are encrypted using TLS 1.2 or higher.
- **At rest:** databases and backups containing customer data are encrypted at rest.
- **Endpoints:** company laptops used to access customer data have full-disk encryption enabled. Contractors are contractually required to use devices with full-disk encryption.

7. Hosting and physical security

- **Data centres:** the hellotax application is hosted by Scaleway SAS in data centres located in France, which apply physical access controls, environmental protections and 24/7 security monitoring.
- **No on-premises servers:** hellotax does not operate its own server rooms; physical security of infrastructure is provided by the hosting provider under its data processing agreement.
- **Offices:** hellotax premises are protected against unauthorised access, and paper documents containing personal data, where used, are stored securely and shredded when no longer needed.

8. Availability, backups and resilience

- **Backups:** automated backups of the hellotax application and its databases are performed daily and retained for 30 days.
- **Backup security:** backups are stored encrypted, within the EEA, and separately from the production environment.
- **Restore testing:** restoration from backups is tested periodically at least annually.
- **Monitoring of availability:** the availability of the hellotax application is monitored continuously, with automatic alerts to the technical team in the event of downtime.

9. Logging and monitoring

- **Logging:** access to production systems and relevant administrative actions are logged. Logs are retained for 90 days and protected against unauthorised modification.
- **Monitoring:** security-relevant events and anomalies are monitored and investigated by the technical team.

10. Secure development and change management

- **Environments:** development, testing and production environments are separated.
- **Test data:** production personal data is not used in development or testing environments
- **Code review:** changes to the hellotax application are reviewed before deployment to production.
- **Patching:** operating systems, frameworks and third-party dependencies are kept up to date, and security updates are applied within a reasonable time according to their severity.

11. Endpoint security

- **Device configuration:** company devices have full-disk encryption, automatic screen lock and up-to-date operating systems.
- **Malware protection:** devices use the built-in or additional malware protection of the operating system.
- **Lost or stolen devices:** loss or theft of a device used to access customer data must be reported immediately and is handled under the incident response procedure.

12. Incident management

- **Procedure:** hellotax maintains a written procedure for detecting, assessing, containing, documenting and notifying personal data breaches.
- **Notification:** affected Customers are notified without undue delay and in any case within 48 hours of hellotax becoming aware of a personal data breach, in accordance with Article 5 of the Agreement.
- **Documentation:** all incidents are documented, including their facts, effects and remedial action, and lessons learned are reflected in the measures.

13. Sub-processor management

- **Due diligence:** before engaging a sub-processor, hellotax assesses its security measures and data protection guarantees (such as certifications, security documentation and data processing agreements).
- **Contracts:** sub-processors are bound by written data processing agreements imposing obligations equivalent to those of the Agreement and, where applicable, by appropriate safeguards for international transfers.
- **Transparency:** the current list of sub-processors is published inside the Hellotax platform and changes are notified in accordance with Article 3 of the Agreement.

14. Data subject rights, return and deletion

- **Data subject requests:** requests received directly from End Users are forwarded to the relevant Customer without undue delay, and hellotax assists the Customer in responding to them.
- **Return and deletion:** upon termination, customer data is returned and deleted in accordance with Article 6 of the Agreement, subject to statutory retention obligations for tax records, during which access to such data is restricted.
- **Secure deletion:** data is deleted from production systems using secure deletion methods and is removed from backups at the end of the backup retention cycle.