This Data Processing Agreement (the "DPA") is entered into between Terahold S.r.l., a single-member company incorporated in Italy, with registered office at Via Francia 21/C, 37135 Verona, Italy, registered with the Verona Companies Register under no. 05234500238, which is also its tax code, REA no. VR-481086, VAT number IT05234500238, share capital EUR 10,000 fully paid, certified email (PEC) terahold@legalmail.it ("Terahold"), and the business customer identified in the Agreement (the "Customer"). Palasil is a trademark used under licence by Terahold S.r.l.

This DPA forms an integral part of the following agreement (the "Agreement"): (a) for a Customer that has accepted the Palasil Terms of Service online (a "Self-service Customer"), the agreement formed by the Terms of Service, this DPA, the Acceptable Use Policy and the other documents referred to in Section 1.2 of the Terms of Service; (b) for a Customer that has signed a Palasil Custom Agreement, that agreement, of which this DPA is one of the contract documents.

This DPA is published in English and in Italian. The prevailing version is set out in Section 19.4.

1. Scope and order of precedence

1.1 This DPA applies to all Processing of Customer Personal Data carried out by Terahold on behalf of the Customer in providing the Service, including, for Customers with a Palasil Custom Agreement, the Managed Services described in the Managed Services Addendum at the end of this DPA (Sections M.1 to M.5).

1.2 For matters concerning the processing of Customer Personal Data, the following order of precedence applies: (a) the SCCs, where they apply under Section 11.3; (b) this DPA, including its Appendices and the Managed Services Addendum; (c) the other documents of the Agreement. Fees, refunds, limitations of liability and termination are governed by the other documents of the Agreement, except where this DPA expressly provides otherwise in Sections 4.5, 10.3, 18 and 19.2.

1.3 This DPA replaces any other terms on the processing of personal data previously agreed between the parties in relation to the Service.

2. Definitions

2.1 The terms "personal data", "processing", "controller", "processor", "data subject", "personal data breach" and "supervisory authority" have the meaning given in Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 (the "GDPR"). In this DPA:

a) "Applicable Data Protection Law" means the GDPR, the Italian Personal Data Protection Code (Legislative Decree no. 196 of 30 June 2003) and any other data protection law applicable to the processing under this DPA;

b) "Customer Personal Data" means the personal data processed by Terahold on behalf of the Customer under the Agreement, as described in Appendix A and, for the Managed Services, in Section M.1.3;

c) "Platform" means the Palasil software service accessible at app.palasil.com, including its AI agent;

d) "Managed Services" means the services that Terahold performs under a Palasil Custom Agreement, with or without the Platform, that is the activities of the Modules, Add-ons and One-off Services ticked in its Order Form;

e) "Service" means the Platform and, for Customers with a Palasil Custom Agreement, also the Managed Services;

f) "Palasil Custom Agreement" means the agreement signed by Terahold and the Customer for the Managed Services, consisting of the Order Form, the General Terms of the Palasil Custom services, the Schedules, this DPA and the other documents listed in it;

g) "Brand Workspace" means the area of the Platform dedicated to a single brand of the Customer, with its Users, content and connections;

h) "User" means a natural person who has access to a Brand Workspace with one of the roles of Owner, Manager, Editor or Analyst; "Owner" means each User with the Owner role, and a Brand Workspace may have more than one Owner;

i) "Connected Tools" means the Klaviyo and Shopify accounts of the Customer connected to the Platform with the Customer's integration keys;

j) "Customer Accounts" means the accounts that the Customer holds on third party platforms, in which Terahold operates to perform the Managed Services under a Palasil Custom Agreement, including the Connected Tools;

k) "Sub-processor" means a third party engaged by Terahold to process Customer Personal Data on behalf of the Customer;

l) "Inference Providers" means the providers of the computing infrastructure that runs the language models used by the Platform, selected through OpenRouter, Inc. under Section 10.4;

m) "Authorised Personnel" means the employees of Terahold and the individual collaborators, who are natural persons, working under the authority of Terahold, who are authorised to process Customer Personal Data and are bound by confidentiality obligations;

n) "Security Incident" means a breach of security of the Service or of the systems of Terahold or of its Sub-processors leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data, and any event that leads Terahold to suspect that an integration key of the Customer has been obtained by an unauthorised person;

o) "SCCs" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission with Implementing Decision (EU) 2021/914 of 4 June 2021;

p) "Subscription" means, for a Self-service Customer, the subscription to the Service for one Brand Workspace under the Terms of Service;

q) "Working Day" means a day from Monday to Friday, other than Italian national public holidays and 21 May (feast of the patron saint of Verona).

2.2 For a Customer with a Palasil Custom Agreement: "Agreement" means the Palasil Custom Agreement; "Order Form" means the Order Form ("Modulo d'ordine") of that agreement; "Terahold" means the party referred to in that agreement as the "Provider" ("Fornitore"); "Customer" means the party referred to in that agreement as the "Customer" ("Cliente"); the Managed Services, the Customer Accounts ("Account Cliente"), the Customer Contacts ("Referenti del Cliente"), the Operational Channel ("Canale Operativo") and the Reserved Operations ("Operazioni Riservate") have the meaning given in that agreement; and the notices that this DPA sends to the Owners are also sent to the Customer Contacts. The Terms of Service do not apply to such a Customer, and the references in this DPA to the Terms of Service apply only to Self-service Customers.

3. Roles of the parties

3.1 The Customer acts as controller of the Customer Personal Data and Terahold acts as processor. Where the Customer acts as processor on behalf of a third party controller, as allowed by Section 8 of the Acceptable Use Policy or by the Palasil Custom Agreement, Terahold acts as sub-processor and the Customer warrants that it is authorised to engage Terahold under this DPA. The Customer informs Terahold in writing of any obligation of its contract with that controller that is stricter than this DPA; such an obligation binds Terahold only if Terahold accepts it in writing.

3.2 Terahold acts as an independent controller for the personal data that it processes to manage its own relationship with the Customer and the security of the Platform, as described in the Palasil Privacy Policy: account and authentication data of Users; invitations, acceptances and signatures of the contractual documents; the records of the "Palasil access" register under Section 6.2; billing data; support requests sent by email to support@palasil.com; the internal records of the administration panel of Terahold and the security logs of the Platform; the inspiration feed. This DPA does not apply to such processing, except that Terahold keeps the "Palasil access" register available to the Customer as provided in Section 6.2. The messages exchanged on Slack as part of the Managed Services are Customer Personal Data processed by Terahold as processor.

3.3 The Connected Tools and the Customer Accounts are services of the Customer, provided under the Customer's own agreements with their providers. Their providers are not Sub-processors of Terahold. The Platform reads data from, and writes data to, the Connected Tools only on behalf of the Customer and as described in Appendix A; Terahold operates in the Customer Accounts only as described in the Managed Services Addendum.

4. Customer instructions

4.1 Terahold processes Customer Personal Data only on the documented instructions of the Customer, including with regard to transfers to third countries, unless required to do so by Union or Member State law to which Terahold is subject. In that case Terahold informs the Customer of that legal requirement before the processing, unless that law prohibits such information on important grounds of public interest.

4.2 The documented instructions of the Customer are:

a) the Agreement and this DPA;

b) the configuration of the Service by the Customer;

c) the actions performed in the Platform by the Users within the permissions of their role, such as connecting a Connected Tool, which includes the instruction to create in the Customer's Klaviyo account the six audience segments described in Appendix A, approving an action proposed by the AI agent, confirming in the chat the creation, described in Appendix A, of a segment proposed by the AI agent, saving a draft in Klaviyo, scheduling or sending a campaign saved in Klaviyo, sending a test email, granting support access under Section 6.1 b) and exporting the data under Section 16.1;

d) the written instructions under Section 4.4.

4.3 Terahold informs the Customer immediately, and in any case within 2 Working Days, if, in its opinion, an instruction infringes Applicable Data Protection Law. Terahold may suspend the execution of that instruction until the Customer modifies it, and is not required to execute it even if the Customer confirms it. The non-execution of such an instruction is not a breach of the Agreement.

4.4 A "written instruction" is a message sent by an Owner by email to support@palasil.com or, under a Palasil Custom Agreement, a message sent by a Customer Contact by email or in the Operational Channel. Where this DPA requires a written instruction for a specific operation, the instruction identifies the operation and, for imports or uploads of lists of persons, the source of the data and the legal basis. Instructions outside the scope of the Agreement are executed only if the parties agree on them in writing, including any fee. Terahold keeps a copy of each written instruction for the term of the Agreement and for 24 months after its termination.

4.5 Terahold informs the Customer within 5 Working Days if, for any reason, it is unable to comply with this DPA. If Terahold breaches this DPA or gives such information, the Customer may instruct Terahold to suspend the processing of the Customer Personal Data concerned until compliance is restored. If compliance is not restored within 1 month of the suspension, or if Terahold does not comply with a final decision of a court or of a supervisory authority concerning its obligations under this DPA, the Customer may terminate the Agreement or, for a Self-service Customer, the Subscriptions concerned, by written notice, with a pro rata refund of the fees paid in advance for the period after termination and without any fee for termination provided in the Agreement.

4.6 The Customer instructs Terahold to derive from the Customer Personal Data, and to use for the purposes of Terahold, only the following aggregated information, which does not identify any data subject:

a) the number of active profiles that Klaviyo counts for the billing of the Customer's Klaviyo account and, for a Customer with a Palasil Custom Agreement, the total value of the orders recorded in the Customer's Klaviyo account in the previous 12 months, to calculate, verify, update and invoice the fees under the Agreement;

b) the results achieved with the Service, expressed as changes and benefits, such as the percentage change of the revenue from emails or the working hours saved, to prepare case studies where the Customer has authorised them under the Agreement;

c) information on the operation of the Service, such as usage volumes, errors and response times, for the improvement and security of the Service.

Terahold does not process Customer Personal Data for any other purpose of its own.

5. Customer obligations

5.1 The Customer is responsible for the lawfulness of the processing it instructs, including: having an appropriate legal basis; providing the information required to data subjects; obtaining and recording the consents of the recipients of its email communications; and complying with the rules on electronic marketing communications. The Customer, as controller, decides whether and how its emails contain tracking pixels or other measurement tools and configures its account at the Connected Tool for that purpose; it provides the recipients with the required information, obtains their consent where required, makes available to them in each email a means to withdraw it, also limited to tracking, and records their choices. The Platform creates drafts in the Customer's Klaviyo account and, on the explicit action of a User whose role allows it or, during a support access under Section 6.1 b), of Authorised Personnel, schedules or sends them; campaigns leave from the Customer's Klaviyo account and the Customer is the sender, whether they are scheduled and sent from the Platform or from Klaviyo, also where Terahold schedules and sends them on the Customer's behalf under the Managed Services.

5.2 The Customer does not submit to the Service special categories of personal data or personal data relating to criminal convictions and offences, and does not use the free text fields of the Service to process such data.

5.3 The Customer enters as recipients of test emails only addresses that it is entitled to use for that purpose, such as those of its own staff.

5.4 Two-step verification is available to all Users and is optional for the Users of the Customer. The Customer decides which persons it invites as Users, with which role, and whether to ask its Users to activate two-step verification.

6. Access by Terahold to the Brand Workspace

6.1 Terahold personnel do not access the content of the Brand Workspace or the Connected Tools, except in the following cases:

a) Managed Services: where the Customer has a Palasil Custom Agreement that includes the Platform, Terahold staff are members of the team of the Brand Workspace with the "Palasil admin" role, identifiable as members of Terahold, and operate in the Customer Accounts within the limits of the Managed Services Addendum;

b) support access: where an Owner, Manager or Editor of the Brand Workspace who is not a member of Terahold personnel grants access to Palasil in the Settings of the Brand Workspace ("Palasil access"), for 3 or 7 days at the User's choice, with the right to revoke it at any time; while the access is active, Authorised Personnel of Terahold may enter the Brand Workspace with the support role after stating the reason for the access and perform in it, in order to handle the request, the actions permitted to the Editor role,

including saving drafts in Klaviyo and scheduling and sending campaigns, excluding the connection and change of the Klaviyo and Shopify keys and the grant of support access; Terahold personnel never grant support access;

c) technical access: where Authorised Personnel access the infrastructure of the Service, including databases and servers, solely for maintenance, security, incident response, fault resolution and the operations under Section 16;

d) legal obligation: where access is required by law or by an order of a competent authority, subject to Section 17.

The automated processing performed by the Platform on the instructions of Section 4.2 is not access by Terahold personnel.

6.2 The "Palasil access" register of each Brand Workspace records:

a) the granting and revocation of support access;

b) each entry of Terahold personnel under Section 6.1 b), with the person, the date and time and the reason;

c) each change made by Terahold personnel to the data of the Brand Workspace during support access, by any means, including the interface of the Platform, the AI agent and the files uploaded to the library: those made through the AI agent with an indication of the change, the others in aggregate form, with one record per type of change every 10 minutes;

d) the drafts saved in or removed from Klaviyo, the segments created in Klaviyo and the schedulings, their cancellation and the sendings of campaigns made by Terahold personnel during support access, with the person, the date and the time;

e) each download of the data under Section 16.1.

Reads, test emails (including the images uploaded to Klaviyo and the assembled preview needed to prepare them), reviews, chat messages, the start of the AI agent (the changes that the AI agent makes are recorded), the refresh of the analytics, the automatic updates of the Platform that do not depend on a choice of Terahold personnel, such as the alignment with Klaviyo and Shopify, and the changes that a person makes to their own data and preferences (profile, notifications, senders pinned in the feed) are not recorded. At the first entry of Terahold personnel under Section 6.1 b), the Owners, Managers and Editors receive a notification in the Platform. Under Section 6.1 a), Terahold staff in the team of the Brand Workspace do not leave a record of each access; the register records, and the Owners receive a notification in the Platform, each time a Palasil admin joins or leaves the team and each time the Brand Workspace passes from Self-service to a Palasil Custom Agreement or vice versa. Owners, Managers and Editors can read the register. Each record is kept for 12 months from its date, also after the deletion of the Brand Workspace, when only Terahold can read it.

6.3 In the internal administration panel, Terahold personnel see, for each Brand Workspace, only service information, such as status, plan, contract, payment status and synchronisation errors, and the list of the persons of the Brand Workspaces with name, email address, role, two-step

verification status and last access, which Terahold processes as controller under Section 3.2. The administration panel does not show the content of the Brand Workspace.

7. Confidentiality

7.1 Terahold ensures that Authorised Personnel are bound by confidentiality obligations, have access to Customer Personal Data only to the extent strictly necessary for their tasks and receive written instructions.

7.2 Individual collaborators of Terahold work only with accounts and tools of Terahold or of the Customer, do not keep their own copies of Customer Personal Data other than working files, which they delete within 7 days of the completion of the task for which they were exported and in any event within 30 days of the export, and are bound by the obligations of Section 10.6.

8. Security

8.1 Terahold implements the technical and organisational measures described in Appendix B, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and the risks for data subjects.

8.2 Terahold may update the measures in Appendix B. No measure is removed or weakened unless it is replaced by a measure offering equal or higher protection.

9. Processing by the AI agent

9.1 To perform the task requested, the AI agent of the Platform sends to language models, through OpenRouter, Inc., the information that the task requires, which may include the Brand kit, the history of the conversation, the results of the tools used by the agent (such as performance indicators, product information, the calendar and the copy of emails) and the text typed by Users, which is sent as written. Images are not sent to the models: the agent selects them on the basis of their file names and product names.

9.2 Requests to the models are subject to the following binding conditions: zero data retention at OpenRouter and at the Inference Providers, which Terahold requests in each request and in the configuration of its OpenRouter account; prohibition of the use of the data for training; exclusion of the providers indicated in Section 10.4. Terahold does not use Customer Personal Data to train or improve AI models.

9.3 The AI agent does not take decisions producing legal effects concerning data subjects or similarly significantly affecting them within the meaning of Article 22 GDPR.

9.4 Terahold includes a machine-readable indication of generation with AI in the HTML of the email drafts generated by the AI agent. To document the origin of the copy generated with AI, Terahold keeps a register of fingerprints (hashes) of each copy and of its sentences, written when the agent writes the copy, when the copy is sent to Klaviyo as a draft and when it is used in a test email. The register contains neither the text of the copy nor the Brand Workspace nor the User, and is kept for 5 years.

9.5 In the Managed Services, Terahold staff may also use the AI assistant listed in Part 2 of Appendix C. The conditions of Section 9.2 do not apply to it; its conditions on retention and training are stated in Appendix C. Terahold sends to the AI image generation systems used in the Managed Services only images of products and texts, never images of identifiable persons or other Customer Personal Data; such systems are not Sub-processors.

10. Sub-processors

10.1 The Customer grants Terahold a general written authorisation to engage Sub-processors. The Sub-processors authorised at the date of this version are listed in Appendix C. The binding list is the one published at palasil.com/legal/subprocessors, with its date and change history, as updated under Sections 10.3 and 10.5. For a Customer with a Palasil Custom Agreement, Appendix C forms part of the signed agreement and its updates follow Section 10.3.

10.2 Terahold imposes on each Sub-processor, by contract, the same data protection obligations as set out in this DPA, as required by Article 28(4) GDPR, and remains fully liable to the Customer for the performance of the Sub-processors' obligations.

10.3 Terahold notifies the Customer of any intended addition or replacement of a Sub-processor listed by name in Appendix C at least 30 days before the new Sub-processor processes Customer Personal Data, by email to the Owners and by updating the published list. Changes to Part 2 of Appendix C are notified only to Customers with a Palasil Custom Agreement. The Customer may object by notice sent within 30 days of Terahold's notice, stating the specific data protection reasons, such as the location of the Sub-processor, a documented security incident or the lack of transfer safeguards. Until the objection is resolved, Terahold does not use the new Sub-processor for the Customer Personal Data or, if this is technically impossible, says so in its reply. If no solution is agreed within 30 days of the objection, the Customer may, by notice sent within the following 15 days, terminate, without penalties and without any fee for termination provided in the Agreement, the Subscriptions for which the Sub-processor is used or, under a Palasil Custom Agreement, the Agreement or the areas of the Managed Services in which the Sub-processor is used, with a pro rata refund of the fees paid in advance for the period after termination. If the Customer does not object or does not terminate within these time limits, the objection is deemed not made or withdrawn.

10.4 Inference Providers are engaged by OpenRouter, Inc., Sub-processor of Terahold, in accordance with the following binding criteria, which Terahold maintains in the configuration of its OpenRouter account:

a) zero data retention, which Terahold also requests in each request;

b) no use of the data for training, whether for paid or free models;

c) exclusion of providers with registered office in the People's Republic of China or controlled by a person or entity established there, of decentralised computing networks and of the other providers specifically excluded by Terahold, which at the date of this version are 20 in total; the list of excluded providers is available on request;

d) headquarters of the provider in the United States or in a country covered by an adequacy decision of the European Commission, as declared by OpenRouter.

Within these criteria the selection of the Inference Provider for each request is made by OpenRouter. For the purposes of this DPA, Inference Providers are Sub-processors and Section 10.2 applies to them. On request to privacy@palasil.com, Terahold informs the Customer, within 15 days, of the Inference Providers that processed the requests relating to its Brand Workspaces, as shown in the request records that OpenRouter makes available to Terahold at the time of the request. Terahold notifies the Customer at least 30 days in advance of any change that makes the criteria less protective; the Customer may object to the change, and terminate, within the time limits and with the effects provided in Section 10.3.

10.5 Terahold may, by simple notice to the Customer, replace the criteria of Section 10.4 with a closed list of Inference Providers listed by name or with the processing of model requests exclusively within the European Union, as these changes increase the level of protection.

10.6 Authorised Personnel, including individual collaborators of Terahold, are not Sub-processors: they process Customer Personal Data as persons acting under the authority of Terahold, within the meaning of Article 29 GDPR and Article 2-quaterdecies of the Italian Personal Data Protection Code, on the written instructions of Terahold and under Section 7. Terahold does not give prior notice of the assignment of Authorised Personnel to the Customer and communicates their names on request. If a supervisory authority or a court qualifies an individual collaborator as a processor, the data protection obligations of the collaboration contract with Terahold apply as the contract under Article 28(4) GDPR and Section 10.2 applies. Companies and professionals that process Customer Personal Data with their own infrastructure are engaged only as Sub-processors under Sections 10.1 to 10.3.

10.7 On request, Terahold provides a copy of the data protection terms agreed with a Sub-processor, from which it may remove trade secrets and other confidential information, or the link to the terms where the Sub-processor publishes them. Terahold notifies the Customer within 5 Working Days of becoming aware that a Sub-processor has breached its data protection obligations in a way that affects Customer Personal Data.

11. International transfers

11.1 Terahold does not transfer Customer Personal Data outside the European Economic Area, except to the Sub-processors listed in Appendix C, to a Customer established outside the European Economic Area, on the basis of an adequacy decision of the European Commission that applies to the Customer or under Section 11.3, and to Authorised Personnel under Section 11.2, and in each case in compliance with Chapter V GDPR, as described in Appendix D.

11.2 Authorised Personnel work from the European Economic Area. A member of Authorised Personnel may access Customer Personal Data from a country outside the European Economic Area, temporarily or permanently, only with the prior written authorisation of Terahold stating the country and the period. In that case: (a) if the country is covered by an adequacy decision of the European Commission, the access is based on that decision; (b) otherwise, for individual collaborators who are not employees of Terahold, Terahold and the collaborator apply the SCCs, Module Three (processor to processor), incorporated in the collaboration contract, after Terahold has assessed the law and practice of the country concerned; (c) Customer Personal Data remain on the systems of the Service and in the Customer Accounts, are accessed remotely with the security measures of Appendix B and are not copied locally, except as

working files deleted within 7 days. Terahold does not authorise access from countries where effective protection of the data cannot be ensured, keeps a record of the authorisations granted and informs the Customer of them on request.

11.3 Where the Customer is established outside the European Economic Area and the disclosure of Customer Personal Data to the Customer is not covered by an adequacy decision of the European Commission that applies to the Customer (for example, a Customer established in the United States that is not on the list of organisations participating in the EU-US Data Privacy Framework), the disclosure of Customer Personal Data by Terahold to the Customer, including access by the Customer's Users from the country where the Customer is established, exports, reports and data entered by Terahold in the Customer Accounts, is governed by Module Four (transfer processor to controller) of the SCCs, with Terahold as data exporter and the Customer as data importer. The text of Module Four of the SCCs, as published in the Official Journal of the European Union L 199 of 7 June 2021, page 31, is incorporated into this DPA by reference and is deemed signed by the parties with the conclusion of the Agreement, without modifications. Appendix E completes the information of Annex I of the SCCs, describes the security measures under Clause 8.2 and sets out the choices under Clauses 17 and 18. In case of conflict, the SCCs prevail.

12. Assistance with data subject requests

12.1 Taking into account the nature of the processing, Terahold assists the Customer by appropriate technical and organisational measures in responding to requests from data subjects. Terahold forwards to the Customer, within 5 Working Days, the requests relating to Customer Personal Data that it receives directly, and does not answer them, except to inform the data subject that the request has been forwarded. Under the Managed Services, Terahold carries out in the Customer Accounts the operations needed to respond to a request on the Customer's written instruction.

13. Security Incidents

13.1 Terahold notifies the Customer within 48 hours after becoming aware of a Security Incident, that is after it has a reasonable degree of certainty that the Security Incident has occurred, by email to the Owners of the Brand Workspaces concerned.

13.2 The notification describes, to the extent known: the nature of the Security Incident, the categories and approximate number of data subjects and records concerned, the likely consequences, the measures taken or proposed and a contact point. Information not yet available is provided in phases without further undue delay.

13.3 In case of suspected compromise of an integration key, Terahold disables its use in the Service and assists the Customer in revoking and replacing the key in the Connected Tool.

13.4 The notification to the supervisory authority and the communication to data subjects, where required, are the responsibility of the Customer, with the assistance of Terahold under this Section. Terahold documents each Security Incident, including its circumstances, consequences and remedial measures.

14. Impact assessments

14.1 Terahold assists the Customer, taking into account the nature of the processing and the information available to it, in its data protection impact assessments and prior consultations relating to the Service, by providing the information on the Service in its possession within 15 days of the request.

15. Audits

15.1 Terahold makes available to the Customer, on request, the information necessary to demonstrate compliance with this DPA and with Article 28 GDPR, including the relevant documentation of its Sub-processors.

15.2 Where the information under Section 15.1 does not answer the Customer's specific written questions, the Customer may carry out an audit, directly or through an independent auditor bound by confidentiality who is not a competitor of Terahold, with the following conditions: not more than once in any 12-month period, except after a Security Incident or at the request of a supervisory authority; with written notice of at least 30 days; between 9:00 and 18:00 Italian time on Working Days; without access to the data of other customers or to information covered by confidentiality obligations of Terahold towards third parties. The Customer bears the costs of the audit, unless the audit reveals a breach of this DPA by Terahold that affects Customer Personal Data.

15.3 On request, the parties make the information under this Section 15, including the results of audits, available to the competent supervisory authority.

16. Export, return and deletion

16.1 During the term of the Agreement, an Owner can download all the data of a Brand Workspace with the "Export all data" function in the Settings of the Platform. The package contains the exportable data in JSON and CSV format, with their metadata, the original files of the library, the description of the structures and formats of the data in Italian and English and a manifest with the SHA-256 fingerprint of each file. For a Brand Workspace that is too large for the function, or on written request of the Customer, Terahold delivers the same package within 10 Working Days of the request.

16.2 After the termination of the Agreement or of a Subscription, the Customer may retrieve the data under Section 16.1 for 30 days (the "Retrieval Period"). The Retrieval Period starts from the termination or, where the Customer has made a switching request, from the end of the transitional period and of any extension under the switching provisions of the Agreement (for Self-service Customers, Section 14 of the Terms of Service; under a Palasil Custom Agreement, Section P.9 of Schedule P). An export request received during the Retrieval Period is fulfilled even if completed after it, and the data are kept until the export is delivered. Within 15 days after the end of the Retrieval Period, or after the delivery of an export requested during it, Terahold deletes the Customer Personal Data from the Service. Backup copies are overwritten in their ordinary rotation within 7 further days. After the deletion Terahold keeps only: (a) the

records of the "Palasil access" register, until 12 months from the date of each record; (b) the data that Terahold must keep under Union or Member State law; (c) the data under Section 16.5. Terahold continues to protect them under this DPA until their deletion.

16.3 The Customer Personal Data stored in the Connected Tools and in the Customer Accounts remain available to the Customer in its own accounts.

16.4 By notice sent before the end of the Retrieval Period, the Customer may choose that Terahold returns the Customer Personal Data before deleting them, by delivering the package under Section 16.1, or that it deletes them earlier. Terahold confirms the deletion by email to the Owners within 10 Working Days of its completion.

16.5 When Terahold receives a written dispute, a formal notice or a request from an authority concerning the Customer, a Brand Workspace or the relationship with the Customer, it may suspend the automatic deletion of the data of the Brand Workspaces concerned that are needed as evidence and keep copies of the chats and of the calendar sends deleted in the meantime, solely to establish, exercise or defend legal claims. For this processing Terahold acts as controller, on the basis of its legitimate interest in the establishment, exercise or defence of legal claims (Article 6(1)(f) and Article 17(3)(e) GDPR). The data are accessible only to Terahold, are not used for any other purpose and are deleted upon the earlier of the following events: the closing of the dispute, the formal notice or the request by agreement, by a final decision or by written waiver; the expiry of the limitation period for the right that is the subject of the dispute or of the formal notice. The ordinary deletion periods then resume.

17. Requests from public authorities

17.1 If Terahold receives a legally binding request from a public authority to access Customer Personal Data, Terahold notifies the Customer, unless prohibited by law, assesses the lawfulness of the request and discloses only the minimum data required. Terahold requires its Sub-processors to handle such requests under their data processing terms, including, where the SCCs apply, Clause 15 of the SCCs.

18. Liability

18.1 The liability of each party under this DPA is subject to the limitations of liability of the Agreement (for Self-service Customers, Section 18 of the Terms of Service; under a Palasil Custom Agreement, Article 20 of the General Terms of the Palasil Custom services), except in case of wilful misconduct or gross negligence, to the extent permitted by Applicable Data Protection Law and without prejudice to the rights of data subjects under Article 82 GDPR.

19. Term and changes

19.1 This DPA remains in force for as long as Terahold processes Customer Personal Data under the Agreement, including the periods of Section 16.

19.2 Terahold may amend this DPA by notice to the Owners sent at least 30 days before the amendment takes effect, stating the amended text and the effective date. An amendment that reduces the protection of Customer Personal Data, including the removal or weakening of a measure of Appendix B or of a criterion of Section 10.4, applies to the Customer only if it

accepts it in writing; if the Customer does not accept it before the effective date, the amendment does not apply to the Customer and either party may terminate the Agreement or, for a Self-service Customer, the Subscriptions concerned, with effect on that date. If the Customer does not accept any other amendment, it may terminate the Agreement or, for a Self-service Customer, the Subscriptions concerned, by notice sent before the effective date, with effect on that date. In both cases the termination takes place without penalties and without any fee for termination provided in the Agreement, with a pro rata refund of the fees paid in advance for the period after termination. An amendment to a clause specifically approved by the Customer under Articles 1341 and 1342 of the Italian Civil Code, or that introduces a clause of that type, applies to the Customer only after its specific written approval. Amendments required by law or by an order of an authority may take effect from the date so required, with notice sent within 5 Working Days of the date on which Terahold becomes aware of the requirement. Updates of the list of Sub-processors follow Sections 10.3 and 10.5 and are not amendments under this Section.

19.3 This DPA is governed by Italian law. The Court of Verona has exclusive jurisdiction over any dispute arising from or relating to this DPA, without prejudice to Section 11.3 and Appendix E for the SCCs and to the rights of data subjects.

19.4 This DPA is available in English and in Italian, with the same version number; each amendment applies to both versions on the same day. The English version prevails, except for Customers with a Palasil Custom Agreement, for whom the version attached to their signed agreement prevails.

19.5 Notices under this DPA are given in writing. Terahold sends them by email to the Owners of the Brand Workspaces concerned and, under a Palasil Custom Agreement, also to the Customer Contacts. The Customer sends notices on personal data to privacy@palasil.com and security reports to security@palasil.com; the other notices follow the notice provisions of the Agreement. An email notice is deemed received when it reaches the recipient's mail server or, if it arrives after 18:00 Italian time or on a day that is not a Working Day, on the next Working Day.

19.6 Terahold publishes each version of this DPA at palasil.com/legal/dpa, with its version number and date; the previous versions remain available in the archive at palasil.com/legal/archive.

Appendix A: Description of the processing

A.1 Parties and roles

Controller: the Customer, as identified in the Agreement. Processor: Terahold S.r.l., Via Francia 21/C, 37135 Verona, Italy, contact for personal data privacy@palasil.com.

A.2 Subject matter, nature, purpose and duration

Terahold processes Customer Personal Data to provide the Service: connection to the Connected Tools; reading and aggregation of data for analysis; creation, when Klaviyo is connected, of six audience segments in the Customer's Klaviyo account, whose names begin with "Palasil ·", based on email consent, clicks, purchases, website visits, bounces and spam complaints, and not on email opens, each created only once; creation in the Customer's Klaviyo account of further audience segments proposed by the AI agent, whose names begin with

"Palasil ·", with rules based on purchases, carts and checkouts, products viewed, website visits, emails received and clicked, email consent and country, and not on email opens, each created only after the confirmation in the chat of a User whose role allows it or of Authorised Personnel in the cases of Section 6.1 a) and b), without changing or deleting segments; generation of plans and email copy by the AI agent; preparation of drafts and test emails in the Customer's Klaviyo account, and scheduling or sending of campaigns from that account, on the instructions of the Users; storage of the content of the Brand Workspace; export of the data; the aggregated information under Section 4.6. The processing for the Managed Services is described in Section M.1.3. Frequency: continuous for the term of the Agreement. Duration: the term of the Agreement and the periods of Section 16.

A.3 Categories of data subjects and personal data

Source or area	Personal data	Data subjects
Shopify	Orders read without the name, email or postal address of the buyer: order value, refunds, shipping country, order number, products ordered. Counts of customer segments, product catalogue and product photos imported into the library. Only aggregated results are stored	Customers of the Customer's store; persons depicted in product photos
Klaviyo	Reports and events associated with the Klaviyo profile identifier, a pseudonymous identifier, used to calculate conversion metrics. Each night the Platform reads the predictive fields of all profiles, such as predicted customer value and churn risk, and stores only aggregated distributions. Open and click metrics are read only in aggregated form per campaign, flow or day: Terahold does not process open events referred to individual profiles, and the segments created by the Platform in the Customer's Klaviyo account are not based on opens. Terahold does not insert tracking pixels in the drafts	Subscribers and customers of the Customer
Brand kit	Information on the brand obtained from Shopify, Klaviyo and the materials supplied by Users	Persons mentioned in the brand materials, if any
Content of the Brand Workspace	Conversations with the AI agent, proposals of the agent and decisions on them, reports on the agent's answers, data of the agent's runs, calendar sends with copy, newsletter HTML, Klaviyo drafts and change requests, Brand kit and its versions, notes, references and templates, monthly plans, reviews and their versions, library folders and files, analysis snapshots and metrics, notifications	Users and persons mentioned in the content or depicted in the images
Team and access	Members of the team and their roles, support access grants (invitations and the "Palasil access" register are processed by Terahold as controller, Section 3.2)	Users and Terahold personnel
Integration keys	Klaviyo and Shopify API keys of the Customer	Not applicable (credentials)
Test emails	Up to 5 email addresses set by the Customer to receive test emails. Test emails are sent through Klaviyo's preview function with a temporary template deleted after sending: no profile is created and no address is added to lists or marked as consenting	Persons whose address is entered by the Customer

Special categories of data: none intended (Section 5.2).

Not processed through the Platform: identified profiles of end customers are not imported into the Platform. When a campaign is scheduled or sent from the Platform, the Platform asks Klaviyo to send it to the audience chosen in the Platform, with any exclusions, and Klaviyo sends it from the Customer's account to the profiles of that audience; the Platform does not receive the profiles of the recipients. The processing under the Managed Services is described in Section M.1.3.

A.4 Retention

Data	Retention
Content of the Brand Workspace and analysis aggregates	Term of the Agreement and Retrieval Period, then deletion under Section 16.2; backup copies overwritten within 7 further days
Working data of the AI agent (runs, events, data read by the tools)	90 days
Analysis snapshots	40 days
Cache of the aggregated Shopify data on the hosting Sub-processor	24 hours
Execution log of the AI agent on the application server, including copies of the system prompt	14 days
Invitations (Terahold as controller, Section 3.2)	30 days after acceptance or expiry
Test email addresses	Until removed by the Customer, and no later than the deletion under Section 16
"Palasil access" register (Terahold as controller, Section 3.2)	12 months from the date of each record, also after the deletion of the Brand Workspace
Logs of the database platform, kept on storage in the European Union	12 months
Requests to language models at OpenRouter and at the Inference Providers	Content not retained (zero data retention); OpenRouter keeps, without content, the metadata of each request, such as time, model, Inference Provider and number of tokens
Register of fingerprints of the copy generated with AI (Section 9.4)	5 years, without text, Brand Workspace or User
Managed Services	As provided in Section M.4

Terahold may suspend the periods above for a Brand Workspace under Section 16.5.

Appendix B: Technical and organisational measures

Access control

1. Access to the Platform only by invitation, sent by email from noreply@palasil.com, with single-use links bound to the email address and valid for 7 days; invitations are deleted automatically 30 days after acceptance or expiry.

2. Two-step verification mandatory for Terahold personnel and available to all Users, with a reminder in the Platform for Users who have not activated it. Where two-step verification is activated, it is also enforced by the database: a session that has not completed it cannot read Customer Personal Data.
3. Roles within each Brand Workspace (Owner, Manager, Editor, Analyst). Write access to the content of a Brand Workspace is restricted by role also at database level; Analysts have read-only access. The text of a chat message can be changed only by its author.
4. Separation between customers through Row Level Security policies in the database, verified with tests before each change to the access rules. Records can reference only objects of the same Brand Workspace.
5. Sensitive actions (deleting or archiving a Brand Workspace, changing integration keys, changing the Owner, removing members, granting support access, and the corresponding administrative actions of Terahold, such as removing two-step verification, inviting or removing administrators, recording payments and changing the contract or the price) require the user to confirm their identity again with the second factor, or with the password where two-step verification is not activated. The confirmation is valid for 10 minutes.
6. Repeated failed sign-in and verification attempts are temporarily blocked: after 10 failed attempts in 15 minutes for the same email address or person, further attempts are refused for 15 minutes.
7. Passwords can be changed only with the current password or through the recovery link sent by email.
8. Access by Terahold to the Brand Workspace only in the cases of Section 6, with the "Palasil access" register.
9. When Terahold support removes the two-step verification of a User, the User is notified in the Platform.

Encryption and secrets

10. Integration keys encrypted with AES-256-GCM and readable only by server-side components.
11. Cookies transmitted only over encrypted connections (HTTPS); the cookies that store the selected Brand Workspace are httpOnly.
12. Separate secrets for each automated component of the Platform; automated jobs authenticated with a secret.
13. Encryption in transit (TLS). Encryption at rest of the database and of the file storage provided by the database Sub-processor.

Storage and location

14. File storage entirely private.

15. Database, authentication and file storage in the European Union (Frankfurt); server functions in the European Union (Frankfurt); application server of the AI agent in the European Union, with restricted access. Some Sub-processors process data outside the European Union, as listed in Appendix C and under the safeguards of Appendix D.

AI processing

16. Zero data retention requested in each request to the language models and set in the configuration of the OpenRouter account; prohibition of training; exclusion of the providers indicated in Section 10.4; images not sent to the models.
17. The tools of the AI agent are limited to an allow list, and its access to files on the application server is confined to its own working folder; the connection to the models accepts only requests with the agent's key.
18. Length limit on each message sent to the AI agent.
19. The AI agent asks the User for confirmation before deleting content or removing a draft from the Customer's Klaviyo account, sets links only to the Customer's own website unless the User provides the address, and does not change the content of an email to make a test email possible.
20. Apart from the six audience segments created when Klaviyo is connected, described in Appendix A, every action that creates or changes content in the Customer's Klaviyo account, such as saving a draft, sending a test email or creating a segment proposed by the AI agent, and every scheduling or sending of a campaign require an explicit action of a User whose role allows it or of Authorised Personnel in the cases of Section 6.1 a) and b). Each draft saved in Klaviyo is recorded with the person who saved it and the time. Each segment proposed by the AI agent is created exactly as proposed, and the confirmation is recorded with the person who gave it and the time; the Platform does not change or delete segments in the Customer's Klaviyo account. A campaign is sent without a scheduled date and time only after a further confirmation of the person who requests the sending, and leaves 3 minutes after that confirmation. The AI agent has no tool to schedule or send campaigns.
21. Machine-readable indication of generation with AI in the HTML of the drafts, and register of fingerprints of the copy generated with AI (Section 9.4).

Availability

22. Daily backup of the database, kept for 7 days.

Organisation

23. Confidentiality obligations and written instructions for all Authorised Personnel, with access based on least privilege, revoked at the end of the engagement.
24. Administrative access to the database and to the servers of the Service reserved to individually identified Authorised Personnel, with separate credentials for each person and for each use. The actions of Terahold personnel in the administration panel are recorded,

as are the entries, changes and operations listed in Section 6.2; the records are kept for 12 months. The logs of the database platform are sent to storage in the European Union, where they are protected from modification and kept for 12 months.

25. Internal procedure for the management of Security Incidents, with a person responsible for it.

26. For the Managed Services, the measures of Section M.3.

Appendix C: Sub-processors

List version 1.0 of 29 October 2026. The current version and its change history are published at palasil.com/legal/subprocessors, and the previous versions of the list remain available in the archive at palasil.com/legal/archive.

Part 1: Service (all Customers)

Sub-processor	Activity	Location	Transfer safeguard
Supabase Pte. Ltd. (Singapore), on Amazon Web Services infrastructure	Database, authentication, file storage	European Union, Frankfurt (eu-central-1); remote access for support possible from third countries	SCCs
Vercel Inc. (United States)	Hosting of the Platform and execution of server functions	European Union, Frankfurt (fra1) for server functions; global network for static content	EU-US Data Privacy Framework and SCCs
Contabo GmbH (Germany)	Application server of the AI agent and connection to OpenRouter; execution log kept for 14 days	European Union	Not applicable
OpenRouter, Inc. (United States)	Routing of requests to language models, with zero data retention	United States	SCCs
Inference Providers, engaged by OpenRouter (Section 10.4)	Execution of language models, with zero data retention and no training	Headquarters in the United States or in countries covered by an adequacy decision; servers possibly in other countries	SCCs through OpenRouter, or adequacy decision
Google, provider of Google Workspace (contracting entity under Google's terms for customers with a billing address in Italy: Google Cloud Italy S.r.l., Milan, Italy)	Email of the Platform sent from noreply@palasil.com, email communications with the Customer and delivery of data exports on request (Google Drive)	Countries where Google and its sub-processors operate, including the United States	Google Cloud Data Processing Addendum: EU-US Data Privacy Framework or SCCs

Sub-processor	Activity	Location	Transfer safeguard
Amazon Web Services EMEA SARL (Luxembourg)	Storage of the logs of the database platform (Amazon S3)	European Union	Not applicable for storage in the European Union; SCCs of the AWS Data Processing Addendum for any transfer outside the European Economic Area

Part 2: Managed Services (only Customers with a Palasil Custom Agreement)

Sub-processor	Activity	Location	Transfer safeguard
Slack Technologies Limited (Ireland), Salesforce group, with Slack Technologies, LLC (United States)	Operational communication and assistance channel with the Customer	Ireland and United States	EU-US Data Privacy Framework (Slack Technologies, LLC is covered by the Salesforce certification) and SCCs of the Salesforce Data Processing Addendum
Anthropic Ireland, Limited (Ireland)	AI assistant used by Terahold staff; no training on the content; standard retention, not zero	United States and other countries outside the European Economic Area	SCCs (Modules Two and Three) incorporated in Anthropic's Data Processing Addendum
n8n GmbH (Germany)	Workflow automations for the Managed Services, where needed to perform them	European Union	Not applicable

Not Sub-processors

Klaviyo, Shopify and the other Connected Tools and Customer Accounts are services of the Customer (Section 3.3). Stripe and the tools used for the inspiration feed process data for which Terahold is controller and are described in the Privacy Policy. The agent orchestration library used by the Platform runs on Terahold's infrastructure and does not transmit data to its developer. Authorised Personnel, including individual collaborators of Terahold, are not Sub-processors (Section 10.6); their names are available on request. The AI image generation systems used in the Managed Services do not receive personal data (Section 9.5).

Appendix D: International transfers

1. Transfers to OpenRouter, Inc. and, through it, to Inference Providers headquartered in the United States are based on the SCCs incorporated in OpenRouter's data processing agreement. Transfers to Inference Providers headquartered in a country covered by an adequacy decision are based on that decision.
2. Transfers to Sub-processors certified under the EU-US Data Privacy Framework are based on the adequacy decision of the European Commission of 10 July 2023 (Implementing Decision (EU) 2023/1795), with the SCCs of their data processing terms as an alternative

safeguard should the certification or the decision cease to apply.

3. Remote access for support by Supabase Pte. Ltd. from third countries is based on the SCCs of Supabase's data processing terms. Transfers to Anthropic Ireland, Limited and to its affiliates outside the European Economic Area are based on the SCCs incorporated in Anthropic's Data Processing Addendum.
4. For the processing of model requests outside the European Union, Terahold has carried out a transfer impact assessment, which takes into account the following measures: zero data retention; prohibition of training; minimisation of the data sent (no images; no names, email or postal addresses of end customers taken from Shopify; Klaviyo profiles referred to only by pseudonymous identifiers); exclusion of the providers indicated in Section 10.4; encryption in transit; the obligations of the importer under Clause 15 of the SCCs.
5. Access by Authorised Personnel from outside the European Economic Area is governed by Section 11.2.
6. Disclosure of Customer Personal Data to a Customer established outside the European Economic Area is based on the adequacy decision of the European Commission that applies to the Customer or, in the cases of Section 11.3, on the SCCs, Module Four, as completed by Appendix E.

Appendix E: SCCs, Module Four (Customers outside the European Economic Area not covered by an adequacy decision)

This Appendix applies only in the cases of Section 11.3. It completes the information required by the Appendix to the SCCs.

E.1 Annex I.A: List of parties

Data exporter: Terahold S.r.l., Via Francia 21/C, 37135 Verona, Italy; contact person for data protection: the legal representative, privacy@palasil.com. Activities relevant to the data transferred: provision of the Service to the Customer under the Agreement. Role: processor. Signature and date: by the conclusion of the Agreement.

Data importer: the Customer, with the name and address indicated in the Agreement and, as contact persons, the Customer Contacts indicated in the Order Form of the Palasil Custom Agreement or, for a Self-service Customer, the Owners. Activities relevant to the data transferred: use of the Service for the email marketing and, where applicable, the other marketing activities of its brands. Role: controller. Signature and date: by the conclusion of the Agreement.

E.2 Annex I.B: Description of the transfer

Item	Description
Categories of data subjects	The data subjects of Appendix A.3 and, for the Managed Services, of Section M.1.3: Users; subscribers, customers and prospects of the Customer; persons mentioned in the content or depicted in images; staff of the Customer in the Operational Channel

Item	Description
Categories of personal data	The personal data of Appendix A.3 and, for the Managed Services, of Section M.1.3
Sensitive data	None intended (Section 5.2)
Frequency	Continuous, for the term of the Agreement
Nature of the processing	Access by the Customer's Users to the Platform from the country of the Customer; delivery of exports, reports and deliverables; entry of data by Terahold in the Customer Accounts on the Customer's instructions; communications in the Operational Channel
Purpose of the transfer and further processing	Provision of the Service to the Customer under the Agreement; the further processing by the Customer is determined by the Customer as controller
Retention	The data received by the Customer are kept by the Customer under its own rules as controller; the data kept by Terahold follow Appendix A.4, Section M.4 and Section 16

Annex I.C (competent supervisory authority) does not apply to Module Four.

E.3 Technical and organisational measures (Clause 8.2)

The measures of Appendix B and, for the Managed Services, of Section M.3 apply to the data processed by Terahold before the transfer and to the transmission of the data.

E.4 Choices under the SCCs

a) Clause 7 (docking clause): not included.

b) Clause 11 (redress): the optional independent dispute resolution body is not selected.

c) Clauses 14 and 15 apply to the extent that Terahold combines personal data received from the Customer with personal data it has collected in the European Union.

d) Clause 17 (governing law): the SCCs are governed by the law of Italy, which recognises the rights of third party beneficiaries (Article 1411 of the Italian Civil Code).

e) Clause 18 (choice of forum and jurisdiction): any dispute arising from the SCCs is resolved by the courts of Italy. Between the parties, the Court of Verona has exclusive jurisdiction. This choice does not limit the rights of data subjects under the SCCs and under the GDPR.

Managed Services Addendum

This Addendum applies only to Customers with a Palasil Custom Agreement. It supplements this DPA, which applies in full.

M.1 Additional processing

M.1.1 For the Managed Services Terahold may, on behalf of the Customer and within the scope of the Order Form:

a) operate in the Customer Accounts, such as email marketing, e-commerce, advertising and social media accounts, through user roles, partner access or integration keys, also with broad read and write permissions granted to ensure the continuity of the Managed Services;

b) process the personal data available in those accounts, including identified profiles of subscribers and customers of the Customer, orders and the related contact details, to the extent necessary for the Managed Services;

c) upload lists of customers to advertising platforms to create custom audiences, only on the Customer's written instruction;

d) process images or videos of real persons supplied by the Customer for the production of content, within the limits of the consent given by those persons;

e) exchange messages and files with the Customer's staff in the Operational Channel, on Slack.

M.1.2 The extent of the technical permissions does not extend the scope of the Managed Services. Terahold uses the permissions only for the Managed Services of the Order Form.

M.1.3 Description of the additional processing, by area of the Managed Services. Each area applies only if activated in the Order Form or if the Order Form includes a service that the Palasil Custom Agreement assigns to that area.

Area	Source and access	Personal data	Data subjects	Operations
A. Email marketing (flows and lead generation, campaigns, consulting and support on Slack)	Customer's email marketing account (for example Klaviyo), with user account and private key with full permissions; for SMS and WhatsApp, also the tool made available by the Customer	Profiles of subscribers and customers (name, email address, phone number, postal address, country), consent status, events and order history, lists and segments, phone numbers for SMS and WhatsApp where active	Subscribers, customers and prospects of the Customer	Creation of segments, flows and campaigns; scheduling and sending of campaigns from the Customer's account under the approval rules of the Palasil Custom Agreement; configuration of sign-up forms on the Customer's instructions; imports of lists only on written instruction stating their source and legal basis; handling of unsubscribes; exports for analysis. Segments or flows based on individual opens, and changes to tracking settings, only on written instruction confirming the legal basis
B. Advertising	Customer's advertising accounts and pages (for example Meta), with partner access; customer lists supplied or exported on instruction	Customer lists (email address, phone number, name, country) uploaded for custom audiences; aggregated campaign statistics	Customers included in audiences; users who interact with ads	Creation of audiences on written instruction; management of campaigns; installation of measurement tools only on written instruction

Area	Source and access	Personal data	Data subjects	Operations
C. E-commerce	Customer's online store (for example Shopify), with staff or collaborator account and the Platform's app	Customer accounts, shipping and billing addresses, orders, returns, consents, reviews; payment instrument data excluded	Customers of the store; authors of reviews	Catalogue and store management; operations on orders and customer records only on written instruction for each operation
D. Content generated with artificial intelligence	Materials supplied by the Customer	Images and videos of real persons; data contained in consents and releases	Persons depicted	Production of content within the limits of the consent of the persons depicted, without the AI image generation systems of Section 9.5; no processing aimed at identifying them
E. Social media	Customer's social media profiles (for example Instagram), with partner or operator access; passwords are shared only where the platform offers no other form of access	Data of followers and of persons who comment, visible in the profile; direct messages visible but not handled	Followers and users who interact with the profiles	Publication of posts and writing of the texts of posts and of the bio; no moderation of comments, no handling of direct messages and no assistance to end customers
F. Consulting	Data shown or shared by the Customer in meetings and in the Operational Channel	Data needed for the analysis requested	Data subjects of the data shared	Analysis and recommendations; no operations in the Customer Accounts other than those of the active areas
All areas	Operational Channel on Slack	Name, role and contact details of the Customer's staff; content of messages and files	Staff of the Customer and persons mentioned	Communication and assistance on the Managed Services

M.1.4 The personal data in the Customer Accounts remain in those accounts. Working files exported from them are kept as provided in Section M.4.

M.2 Reserved operations

M.2.1 Terahold carries out the Reserved Operations, which include the permanent deletion of data of end customers, the import of contacts or the recording of their consent, the insertion of scripts, pixels or other tracking tools and the transmission of personal data of end customers to persons other than Terahold, its Sub-processors and the Customer Accounts already

connected, only on a written instruction of a Customer Contact that identifies them, as provided in the Palasil Custom Agreement. The permanent deletion of data of end customers to respond to the requests of data subjects under Section 12.1 also requires such an instruction. Recording unsubscribes and objections does not require an instruction.

M.3 Staff and Authorised Personnel

M.3.1 Where the Palasil Custom Agreement includes the Platform, Terahold staff working on the Managed Services are members of the team of the Brand Workspace with the "Palasil admin" role, exclusively with an email address of the domains palasil.com or terahold.com, identifiable as members of Terahold. They are Authorised Personnel under Section 10.6 and are bound by confidentiality and by security obligations proportionate to their level of access, including two-step verification, the use of a password manager and the deletion of working files within 7 days of the completion of the task for which they were exported and in any event within 30 days of the export.

M.4 Sub-processors, retention and end of the Managed Services

M.4.1 The Sub-processors of Part 2 of Appendix C apply. Working files exported from the Customer Accounts are deleted as provided in Section M.3.1. The channels dedicated to the Customer in Terahold's Slack workspace are kept for the term of the Managed Services and deleted within 30 days of their end; before deleting them, Terahold extracts from them a copy of the written instructions and of the approvals exchanged in them, which it keeps for the period stated in Section 4.4. The content processed with the AI assistant of Appendix C is kept under the conditions stated there.

M.4.2 Within 5 Working Days after the end of the Managed Services, Terahold: (a) removes its staff from the team of the Brand Workspace, if any, and, where its permissions allow, from the Customer Accounts; (b) stops using all keys and accesses granted; (c) informs the Customer in writing of the roles, partner accesses and keys that only the Customer can revoke. Terahold remains liable for any use of those accesses by its staff. If the Customer continues to use the Platform without Managed Services, this DPA continues to apply without this Addendum.

M.5 Authorised Personnel outside the European Economic Area

M.5.1 Section 11.2 applies to the Managed Services.