Data Processing Agreement
Applicable to cPanel Partners and Direct Customers of WebPros International LLC

This Data Processing Agreement (this "Agreement" or this "DPA") governs the Processing of Personal Data by WebPros on behalf of cPanel partners and direct cPanel customers (each a "Customer" or the "Data Controller").

The Customer obtains the products and services to which this Agreement relates from WebPros International LLC, 1100 W 23rd St, Houston, TX 77008, United States of America ("WebPros International LLC"). This Agreement forms an integral part of, and is incorporated by reference into, the agreement between the Customer and WebPros International LLC under which those products and services are provided, including the applicable terms of service, end user license agreement, partner agreement or any other contractual understanding between the Customer and WebPros International LLC which involves the Processing of Personal Data on behalf of the Customer (collectively the "Base Agreement").

Within the WebPros group of companies, WebPros International GmbH, Vordergasse 59, 8200 Schaffhausen / Switzerland (hereinafter referred to as "WebPros" or the "Data Processor"), is the legal entity responsible for data protection matters. WebPros International GmbH therefore acts as the Data Processor under this Agreement and assumes the obligations of the Data Processor set out herein for and on behalf of WebPros International LLC and of the further WebPros entities which are involved in the provision of the products and services and which are listed in Exhibit 3.

The Data Controller and the Data Processor are each referred to as a "Party" and collectively as the "Parties" hereto.

This Agreement does not require separate execution and applies without a signature by either Party. It applies to each Customer as from the date on which the Base Agreement takes effect, provided and to the extent that the Data Processor Processes Personal Data on behalf of the Data Controller. The Data Controller is identified by the account and contract data recorded for it under the Base Agreement.

This Agreement specifies the Parties' data protection obligations according to Art. 28 General Data Protection Regulation ("GDPR") in regards to the Processing of personal data by the Data Processor on behalf of the Data Controller under the Base Agreement. It applies to all activities performed in connection with the Base Agreement in the course of which the Data Processor, or a 3rd party acting on its behalf (the "Sub-Processor"), may come into contact with or process personal data belonging to the Data Controller or its' customers on behalf of the Data Controller. The applicability of this Agreement is conditioned upon the existence of a data processing activity performed by the Data Processor on behalf of the Data Controller. In the absence of such processing activity, this Agreement will not apply.

This Data Processing Agreement comes into force and effect on the date on which the Base Agreement takes effect (the "Effective Date") and remains in force for as long as the Data Processor Processes Personal Data on behalf of the Data Controller under the Base Agreement. It cannot be terminated independently of the Base Agreement. This Agreement will terminate automatically at the termination or expiry of the Base Agreement, provided that §3(4), §3(7), §4(3) and §10 survive such termination for as long as the Data Processor holds any Personal Data of the Data Controller and, in respect of §10, for the applicable statutory limitation period. All Exhibits hereto form integral parts of this Data Processing Agreement.

§1 Definitions

(1) "Personal Data"
Personal Data means any information relating to an identified or identifiable natural person (the "Data Subject").

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

(3) "Instruction"
Instruction means any written instruction, issued by the Data Controller to the Data Processor, and directing the same to perform a specific action with regard to Personal Data (including, but not limited to, de-personalizing, blocking, deletion, making available). Instructions will initially be specified in the Base Agreement and may, from time to time thereafter, be amended, amplified or replaced by Controller in separate written instructions (individual instructions).

(4) "Data Controller"
Data Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

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

(6) "GDPR"
GDPR means the EU General Data Protection Regulation 2016/679.

(7) "EU Standard Contractual Clauses" or "EUSCC" means a set of contractual clauses for data transfers from controllers in the EU to processors established outside the EU or EEA, as issued by the European Commission (Decision C (2021) 3972).

(8) This Agreement applies to the Processing of Personal Data by WebPros on behalf of the Customer in the course of providing Services under the Base Agreement. For the purposes of this Data Processing Agreement:

The Customer may in some cases be considered as a Data Processor for a third-party Data Controller, and WebPros may in such situations be a Sub-Processor to Process Personal Data on the Customer's behalf. For simplification purposes, WebPros is hereinafter referred to as a Data Processor and the Customer is hereinafter referred to as a Data Controller. Any notifications given by the third -party Data Controller to the Customer will in such cases be conveyed to WebPros insofar as the notifications relate to the Services provided by WebPros. In addition, any instructions given by the Customer to WebPros relating to the Processing of Personal Data should not in such cases contradict or conflict with the instructions given by the third-party Data Controller.

§ 2 Scope and Responsibility

(1) The provisions of this DPA shall apply whenever the Data Processor, in the course of its main contractual services, gains access to personal data (hereinafter referred to as 'Data') for which the Data Controller is responsible within the meaning of data protection law. In these cases, the Data Processor processes data on behalf of and in accordance with the instructions of the Data Controller within the meaning of Article 28 GDPR (contract data processing).

The Data Controller remains the controller in the sense of data protection law. The Data Controller is responsible for compliance with all data protection requirements, in particular the GDPR, but also for ensuring that the legal rights of data subjects in connection with personal data are observed.

(2) The data processing by the Data Processor is carried out in the manner, scope and for the purpose specified in **Exhibit 1** to this Agreement; the processing concerns the types of personal data and categories of data subjects specified therein. The duration of the processing corresponds to the term of the Base Agreement.

(3) The Data Processor may aggregate Personal Data into statistical or technical data that does not permit the identification of any Data Subject by any means reasonably likely to be used, and may use such aggregated data for the purposes of securing, operating, maintaining, troubleshooting and capacity-planning the Services. The Data Processor will not use Personal Data, or data derived from it, to train, fine-tune or otherwise improve any machine learning or artificial intelligence model, and will not disclose it to any third party for that purpose, unless the Data Controller has given prior separate written consent. Any use of data for purposes determined by the Data Processor itself falls outside the scope of this Agreement, and the Data Processor acts as an independent controller in respect of such use.

(4) Data processing by the Data Processor shall generally take place within the European Union (EU) or in another country that is a party to the Agreement on the European Economic Area (EEA). Nevertheless, the Data Processor is also permitted to process Data Controller data outside the EEA in compliance with the provisions of this contract, provided that the Data Processor informs the Data Controller in advance of the location of the data processing and the requirements of Articles 44 to 49 GDPR are met. The Data Processor will not rely on a derogation under Article 49 GDPR for transfers that are repetitive or that form part of the regular provision of the Services.

§ 3 Obligations of Processor

(1) The Data Processor will collect, process and use Personal Data only in compliance with and within the scope of the Data Controller's Instructions or as specified and agreed in the Base Agreement.

(2) Within the Data Processor's area of responsibility, the Data Processor will structure its internal corporate organization for compliance with the specific requirements of the protection of Personal Data, established by GDPR, local data protection laws or any other applicable privacy and data protection laws and regulations currently in effect (the "Data Protection Laws"). The Data Processor will take the appropriate technical and organizational measures to ensure a level of security appropriate to the risk to the Data Controller's Personal Data in accordance with the requirements of Article 32 GDPR. The current measures are set forth in **Exhibit 2** hereto. Such measures hereunder will include, but not be limited to:

a) the pseudonymization and encryption of personal data where possible;
b) the ability to ensure ongoing confidentiality, integrity, availability and resilience of Processing systems and services (logical, physical access control, transfer control);
c) the ability to restore availability and access to personal data in a timely manner in the event of a physical or technical incident (availability control);
d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures for ensuring the security of the Processing.

Data security measures referred to in this section above will be supported by the use of state-of-the-art encryption technology.

(3) Upon the Data Controller's request, the Data Processor will provide all information concerning the protection of Personal Data within the Data Processor's organization in the sense of Article 32 of GDPR and will provide reasonable assistance to the Data Controller in order to allow it to comply with its obligations under the Data Protection Laws.

(4) The Data Processor will ensure that any personnel, entrusted with Processing the Data Controller's Personal Data have undertaken in writing to comply with the principle of integrity and confidentiality in accordance with Article 5(1)(f) GDPR and have committed themselves to confidentiality in accordance with Articles 28(3)(b), 29 and 32(4) GDPR. The undertaking to secrecy will continue after the termination of the above-entitled activities.

(5) The Data Processor will notify the Data Controller of the contact details of the Data Processor's data protection Officer (if appointed) or the responsible associate, respectively.

(6) The Data Processor will inform the Data Controller of any Personal Data Breach (as defined in Article 4(12) GDPR) without undue delay and in any event within forty-eight (48) hours of becoming aware of it. The notification will be sent to the contact details recorded for the Data Controller under the Base Agreement, or to such other contact address as the Data Controller has notified to the Data Processor in text form,

and will describe, to the extent known at the time and supplemented without undue delay thereafter: the nature of the breach and the categories and approximate number of Data Subjects and records concerned; the likely consequences; and the measures taken or proposed to address the breach and mitigate its effects. The Data Processor will investigate and document the breach and provide reasonable cooperation to enable the Data Controller to meet its obligations under Articles 33 and 34 GDPR. The Data Processor will not notify any supervisory authority or Data Subject in respect of a Personal Data Breach affecting the Data Controller's Personal Data unless required by law or instructed by the Data Controller.

(7) Where applicable, the Data Controller will retain title as to any carrier media provided to the Data Processor as well as any copies or reproductions thereof. The Data Processor will store such media safely and protect them against unauthorized access by third parties. The Data Processor will, upon the Data Controller's request, provide to the Data Controller all information on the Data Controller's Personal Data and information. The Data Processor will be obliged to securely delete any test and scrap material, based on an Instruction issued by the Data Controller on a case-by-case basis. Where the Data Controller so decides, the Data Processor will hand over such material to the Data Controller or store it on the Data Controller's behalf.

(8) The Data Processor will immediately inform the Data Controller if, in the Data Processor's opinion, an Instruction infringes the GDPR, the Swiss Federal Act on Data Protection or any other applicable Data Protection Law. The Data Processor may suspend execution of the affected Instruction until the Data Controller confirms or amends it in writing.

(9) Taking into account the nature of the Processing and the information available to it, the Data Processor will provide reasonable assistance to the Data Controller in ensuring compliance with the Data Controller's obligations under Articles 32 to 36 GDPR, including in carrying out data protection impact assessments and in any prior consultation with a supervisory authority. The Data Processor may charge its then-current professional services rates for assistance that goes materially beyond providing information already documented in Exhibit 2 or in the Data Processor's current security documentation.

(10) The Parties acknowledge that, in the course of the support services described in Exhibit 1, the Data Processor may obtain visibility of Personal Data whose categories it does not determine and which may include special categories of Personal Data within the meaning of Article 9 GDPR. The Data Processor will not Process such data beyond what is necessary to perform the requested support, will restrict such access to authorised support personnel and to the duration of the support request, and will not extract, copy or retain such data on its own systems except where the Data Controller has instructed it to do so. The Data Controller will avoid providing the Data Processor with access to special categories of Personal Data where the requested support can reasonably be performed without such access.

§ 4 Obligations of Controller

(1) The Data Controller and Data Processor each will be responsible for conforming with such statutory data protection regulations as are applicable to them.

(2) The Data Controller is responsible for notifying Personal Data Breaches to the competent supervisory authority under Article 33(1) GDPR and to Data Subjects under Article 34 GDPR. The Data Processor's obligation is to notify the Data Controller in accordance with Article 33(2) GDPR and §3(6) of this Agreement.

(3) Upon termination or expiry of the Base Agreement the Data Controller will, by way of an Instruction, stipulate whether the Personal Data is to be returned or deleted, and the Data Processor will comply within a reasonable period set by the Data Controller. If the Data Controller has issued no such Instruction within sixty (60) days of termination or expiry, the Data Processor will delete the Personal Data, including existing copies, and will confirm the deletion in writing upon request. Personal Data contained in routine backups will be deleted in accordance with the Data Processor's documented backup rotation cycle. The Data Processor may retain Personal Data to the extent and for as long as required by applicable law, in which case it will continue to protect that data in accordance with this Agreement and will Process it solely for the purpose of complying with that requirement.

(4) The Data Controller is responsible for the lawfulness of the Processing it instructs and for the lawfulness of the Personal Data it provides to the Data Processor. Should third parties assert claims against the Data Processor arising from the Data Controller's Instructions or from the Personal Data provided by the Data Controller, the Data Controller will indemnify the Data Processor against such claims, including reasonable legal costs, except to the extent the claim is caused by a breach of this Agreement by the Data Processor, by Processing outside the Data Controller's Instructions, or by the Data Processor's negligence or wilful misconduct. This paragraph does not affect either Party's liability under Article 82 GDPR.

(5) It is the Data Controller's responsibility to provide the Data Processor with the data in timely manner for the provision of services under the main contract and the Data Controller is responsible for the quality of the Data Controller's data. The Data Controller shall inform the Data Processor immediately and in full if the Data Controller discovers errors or irregularities with regard to data protection provisions or the Data Controller's instructions when checking the results of the Data Processor's work.

(6) Each Party maintains its own record of processing activities as required by Article 30 GDPR. The Data Controller will provide the Data Processor, upon request, with such information as the Data Processor reasonably requires to maintain its record under Article 30(2) GDPR and which is not already available to it.

(7) Where the Data Processor receives a legally binding request from a public authority for disclosure of the Data Controller's Personal Data, §9 of this Agreement applies. The Data Controller will provide the Data Processor with such reasonable assistance as the Data Processor requires in order to respond to the request, provided that nothing in this paragraph obliges either Party to facilitate a disclosure that is not required by applicable law.

(8) Any additional cost arising in connection with the return or deletion of Personal Data after the termination or expiration of the Base Agreement or arising out of Instructions outside the Base Agreement's scope shall be borne by the Data Controller.

(9) If applicable, the Data Controller will at all times make sure to have a sufficient legal basis for handing over his own customers' data to the Data Processor in the event, the processing activities of the Data Processor relate to customers' data. Such legal basis has to be set forth in writing between the Data Controller and his customer and must be provided to the Data Processor upon request.

(10) The Data Controller will maintain complete and up to date contact details in its account under the Base Agreement and will, where it has appointed a data protection officer or another contact for data protection matters, notify those contact details to the Data Processor. Notices and information given by the Data Processor to the contact details so recorded are deemed to have been validly given to the Data Controller.

§ 5 Enquiries by Data Subjects or Supervisory Authorities

The Data Processor will, without undue delay, inform the Data Controller of any request, claim or notice received from a Data Subject, a supervisory authority or any other third party which relates to the Processing of the Data Controller's Personal Data. The Data Processor will not respond to such a request itself, except to confirm receipt, to refer the requester to the Data Controller, or where it is legally required to respond.

Taking into account the nature of the Processing, the Data Processor will assist the Data Controller by appropriate technical and organizational measures in fulfilling the Data Controller's obligations to respond to requests by Data Subjects exercising their rights under Articles 12 to 22 GDPR, including the rights of access, rectification, erasure, restriction of Processing, data portability and objection, and in providing the information required under Articles 13 and 14 GDPR. Where the requested assistance materially exceeds making available functionality already provided in the Services, the Data Processor may charge its then-current professional services rates.

§ 6 Audit Obligations

The Data Controller may, prior to the commencement of Processing, and in regular intervals thereafter, audit the technical and organizational measures taken by the Data Processor, and will document the resulting findings. For such purpose the Data Processor will make available to the Data Controller all information necessary to demonstrate compliance with this Agreement and with Article 28 GDPR.
The Data Controller will: (i) ensure that any information request, audit or inspection is undertaken within normal business hours (unless such other time is mandated by a competent data protection regulator) with minimal disruption to Data Processor's and/or its Sub-Processors' businesses, and acknowledging that such information request, audit or inspection: (a) will not oblige Data Processor to provide or permit access to information concerning Data Processor's internal business information or relating to other recipients of services from the Data Processor; and (b) shall be subject to any reasonable policies, procedures or instructions of Data Processor or its Sub-Processors for the purposes of preserving security and confidentiality; and (ii) provide Data Processor at least 30 days' prior written notice of an information request and/or audit or inspection (unless the competent data protection regulator provides Data Controller with less than 30 days' notice, in which case Data Controller shall provide Data Processor with as much notice as possible).

The Data Processor will ensure that its agreements with Sub-Processors grant audit and information rights equivalent to those in this §6, and will exercise those rights on the Data Controller's behalf where a direct audit of the Sub-Processor is not practicable.

The Data Processor may satisfy an information request or audit in the first instance by providing its current security documentation, together with a written response to the Data Controller's questions. An on-site inspection may be requested where those materials do not reasonably address the request.

A maximum of one information request, audit and/or inspection may be requested by Data Controller in any twelve (12) month period unless an additional information request, audit and/or inspection is mandated by a competent data protection regulator in writing or follows a Personal Data Breach affecting the Data Controller's Personal Data.

The Data Processor will cooperate with the Controller in the sense of Article 28(3)(h) GDPR in the facilitation of any audit or inspection or other work undertaken pursuant to Data Processor's obligations under this Agreement.

§ 7 Sub-Processors, Subcontractors

(1) The Data Controller generally agrees that the Data Processor may subcontract parts of its contractual obligations hereunder to the Data Processor's affiliated companies and/or third parties (Sub-Processors) within or outside the EEA. Sub-Processors will only act on the Data Processor's Instructions when Processing Personal Data and will abide by any applicable data protection laws in effect. The Data Processor agrees and warrants to remain liable to the Data Controller for any acts or omissions of its Sub-Processors related to the subcontracted Processing by them under this Agreement.

(2) Where the Data Processor engages Sub-Processors, the Data Processor will be obliged to pass on the Data Processor's contractual obligations hereunder as required by the GDPR to such Sub-Processors and will restrict the Sub-Processor's access to data only to what is necessary to provide and maintain the subcontracted services. Sentence 1 of this paragraph 2 will apply in particular, but will not be limited to, the contractual requirements for confidentiality, data protection and data security stipulated between the parties of the Base Agreement. Furthermore, the Data Processor is responsible for setting-up and maintaining appropriate safeguards between it and the Sub-Processors as stipulated in Article 46 GDPR.

(3) The list of Sub-Processors in **Exhibit 3** hereto lists all Sub-Processors that are currently authorized by WebPros entities for specific purposes. Depending on the Service requested, only specific Sub-Processors may be involved in the Processing of certain data. WebPros will periodically update the applicable list of Sub-Processors on its websites. The Data Processor offers a free and automatic update service (https://www.webpros.com/legal/#gdpr) in order to keep the Data Controller reasonably informed about any changes to this list. In addition, the Data Controller hereby commits to periodically check such website for changes in the list of WebPros Sub-Processors and acknowledges that satisfies its needs in regards to Sub-Processor information by the Data Processor. Via that update service the Data Processor will announce any intended addition of a Sub-Processor that Processes Personal Data in a country outside the EEA, the United Kingdom or Switzerland which is not covered by an adequacy decision, at least fourteen (14) days before that Sub-Processor begins Processing.

If the Data Controller objects to a newly added Sub-Processor on reasonable data protection grounds within thirty (30) days of the relevant change being published in the list of Sub-Processors referred to in paragraph (3), the Parties will discuss the objection in good faith. If no resolution is reached within a further thirty (30) days, the Data Controller may (i) reject a specific form of data Processing in writing, or (ii)

terminate the affected Services under the Base Agreement without penalty, against pro rata refund of prepaid fees for the terminated Services. The Data Processor has no right to terminate this Agreement independently of the Base Agreement.

§ 8 International Data Transfers

The Data Controller acknowledges that the Data Processor and its Sub-Processors may Process Personal Data outside the EEA, the United Kingdom or Switzerland. Any such transfer will be subject to an appropriate transfer mechanism under Chapter V GDPR.

Where the EU Standard Contractual Clauses are the appropriate mechanism for a transfer under this Agreement, the EUSCC are hereby incorporated into this Agreement by reference and form Exhibit 4, with Module Two (transfer controller to processor) applying, or Module Three (transfer processor to processor) applying where the Data Controller acts as a processor on behalf of a third-party controller. Exhibit 1 serves as Annex I.B, Exhibit 2 as Annex II and Exhibit 3 as Annex III to the EUSCC. The docking clause (Clause 7) applies.

For transfers subject to the Swiss Federal Act on Data Protection, the EUSCC apply with the amendments recognized by the Federal Data Protection and Information Commissioner. For transfers subject to United Kingdom data protection law, the International Data Transfer Addendum issued under s.119A of the Data Protection Act 2018 applies to the EUSCC.

Where the Data Processor relies on an adequacy decision or on a certification under the EU-US or Swiss-US Data Privacy Framework and that decision or framework is invalidated, suspended or ceases to cover the relevant transfer, the EUSCC as incorporated above will apply automatically from that date without any further action by either Party.

§ 9 Duties to Inform

Where the Data Controller's Personal Data becomes subject to search and seizure, an attachment order, confiscation during bankruptcy or insolvency proceedings, or similar events or measures by third parties, public authority or government body, while being Processed, the Data Processor will inform the Data Controller without undue delay. The Data Processor will, without undue delay, notify to all pertinent parties in such action, that any Personal Data affected thereby is in the Data Controller's sole property and area of responsibility, that Personal Data is at the Data Controller's sole disposition, and that the Data Controller is the responsible body in the sense of the GDPR and if possible, the Data Processor will not disclose any Personal Data of the Customer to the extent allowed by the applicable laws.

Where the Data Processor receives a legally binding request from a public authority, including a judicial authority, for disclosure of the Data Controller's Personal Data, the Data Processor will: (i) notify the Data Controller of the request without undue delay, unless prohibited by applicable law, and in that case use reasonable efforts to obtain a waiver of the prohibition; (ii) assess the legality of the request and, where it concludes that there are reasonable grounds to consider the request unlawful under applicable law, challenge it, including by seeking interim measures, and pursue available avenues of appeal; (iii) disclose only the minimum amount of Personal Data permissible in responding to the request; and (iv) document its assessment and any disclosure made, and make that documentation available to the Data Controller. The Data Processor will not disclose Personal Data to a public authority voluntarily.

§10 Indemnity and Limitation of Liability

(1) Unless expressly stipulated differently in this Agreement, the Base Agreement or the applicable law, the Data Processor is solely liable and responsible for its' gross negligence and willful misconduct, in each case to the extent such limitation is permitted under the applicable law. This limitation of liability also applies to its assigned agents and proxies. In cases of simple negligence, the Data Processor shall only be liable for typical and foreseeable damages, caused by a violation of a cardinal contractual obligation. In this case, however, the Data Processor's, its affiliates', officers', directors', employees', agents', service providers', suppliers' or licensors' liability for indirect damages, business interruption, loss of goodwill or for any type of incidental, special, exemplary, consequential or punitive loss or damages is excluded, regardless of whether such Party has been advised of the possibility of such damages and if such exclusion is permitted under the applicable law.

(2) Notwithstanding the foregoing, in the event the Data Controller forwards his own customers' data to the Data Processor for further processing under this Agreement, the Data Controller will indemnify and hold harmless the Data Processor against all claims made by third parties, cost (including legal costs) and fines relating to the legal basis of such data forwarding. In this respect, the Data Controller has the sole and exclusive responsibility of making sure to have sufficient permission by the Data Subject or his customers and a legal basis to forward data to WebPros for processing. WebPros strictly disclaims all associated liability towards Data Subjects or Data Controller customers, respectively.

(3) Notwithstanding anything to the contrary in this Agreement or the Base Agreement, the Data Processor's aggregate liability to the Data Controller or any 3rd party arising out of this Agreement or any data Processing services performed hereunder shall in no event exceed the limitations set forth in the Base Agreement, provided that those limitations do not apply to liability for willful misconduct, to liability for breach of the confidentiality obligations under §3(4), or to the extent liability cannot be limited under the applicable law. For the avoidance of doubt, this section shall not be construed as limiting the liability of either party with respect to claims brought by Data Subjects. Article 82(4) GDPR applies to claims brought by Data Subjects, and the internal allocation of liability between the Parties follows Article 82(5) GDPR.

(4) The Data Processor shall be entitled to disclose details of the Data Controller's instructions and the data Processing carried out for the purpose of exempting itself from liability pursuant to Art. 82 (3) GDPR. The Data Controller shall do everything necessary to enable the Data Processor to release itself from liability to third parties in this context.

§11 Artificial Intelligence

(1) Where the Services include features that use artificial intelligence or machine learning systems, including large language models provided by the Sub-Processors identified as AI Sub-Processors in Exhibit 3, the Data Processor Processes Personal Data in connection with those features solely on the Data Controller's Instructions and for the purposes described in Exhibit 1.

(2) The Data Processor will not use, and will contractually require its AI Sub-Processors not to use, the Data Controller's Personal Data, prompts, inputs or outputs to train, fine-tune or otherwise improve any general-purpose or other artificial intelligence model, unless the Data Controller has given prior separate written consent.

(3) The Data Processor will not use the Services to make decisions based solely on automated processing which produce legal effects concerning a Data Subject or similarly significantly affect a Data Subject within the meaning of Article 22 GDPR, unless expressly instructed to do so by the Data Controller.

(4) The Parties acknowledge that, in respect of artificial intelligence systems made available as part of the Services, the Data Processor may act as a provider and the Data Controller as a deployer within the meaning of Regulation (EU) 2024/1689 (the "AI Act"). The Data Processor will provide the Data Controller with the information reasonably required to enable the Data Controller to comply with its transparency obligations under Article 50 of the AI Act, and will inform the Data Controller of the AI Sub-Processors involved by way of the list referred to in §7(3).

(5) Personal Data transmitted to an AI Sub-Processor is subject to §7 and §8 of this Agreement and to the safeguards recorded in Exhibit 3. Exhibit 1 identifies, per product, whether artificial intelligence features involve the Processing of Personal Data.

§12 General, Choice of Law

(1) No change of or amendment to this Agreement and all of its components, including any commitment issued by the Data Processor, will be valid and binding unless agreed between the Parties in text form and unless they make express reference to being a change or amendment to these regulations. The foregoing will also apply to the waiver of this mandatory form requirement. The foregoing does however not apply to updates of the list of Sub-Processors in Exhibit 3, which are made in accordance with §7(3), and it does not apply to amendments of this Agreement which the Data Processor publishes in order to reflect changes in applicable data protection law or in the binding guidance or decisions of competent supervisory authorities or courts. The Data Processor publishes the then current version of this Agreement on the cPanel website. Amendments published in accordance with sentence 3 take effect thirty (30) days after their publication, provided that no such amendment will reduce the level of protection afforded to the Personal Data Processed on behalf of the Data Controller.

(2) If any provision (or part thereof) of this Agreement is held invalid by a court with jurisdiction over the Parties, such provision (or part thereof) will be deemed to be restated to reflect as far as possible the Parties' original intentions in accordance with applicable law, and the remainder of the Agreement or provision will remain in full force and effect as if the Agreement had been entered into without the invalid provision (or part thereof).

(3) This Agreement is governed by the laws of Switzerland. The courts located in Zürich / Switzerland will have the exclusive jurisdiction over the parties in regards to this Agreement. Notwithstanding the foregoing choice of law, the Parties expressly agree to make the terms of GDPR applicable to this Agreement.

(4) Name of the WebPros External Data Protection Officer: Vary.Legal GmbH (privacy@webpros.com)

(5) Representative pursuant to Article 27 GDPR: WebPros Germany GmbH, Hohenzollernring 72, 50672 Cologne, Germany, acts as the representative of WebPros International GmbH in the Union within the meaning of Article 27 GDPR. Data Subjects and supervisory authorities may address the representative on all issues related to the Processing under this Agreement.

(6) Swiss Federal Act on Data Protection. Where and to the extent the Processing is subject to the Swiss Federal Act on Data Protection of 25 September 2020 (the "FADP"), the following applies in addition: references to Personal Data include data relating to legal entities to the extent protected under the FADP. The Data Processor may engage a Sub-Processor only with the authorisation of the Data Controller, which is given by way of the general authorisation in §7 and the list in Exhibit 3. The Data Processor will notify the Data Controller of any Personal Data Breach in accordance with §3(6) so as to enable the Data Controller to meet its obligation under Article 24 FADP to notify the Federal Data Protection and Information Commissioner as soon as possible. Disclosures of Personal Data abroad are subject to Articles 16 and 17 FADP, with the mechanisms set out in §8 and Exhibit 4 applying accordingly.

(7) United States state privacy laws. Where and to the extent the Processing is subject to a United States state privacy law, Exhibit 5 applies in addition to this Agreement.

Exhibit 1

A description of Personal Data elements and the purpose of their Processing by the Data Processor on behalf of the Data Controller per product. The description will state the extent, the nature and purpose of contemplated collection, Processing and use of data, the type of data, and the circle of data subjects.

Product	Categories of Data Subjects	Categories of Personal Data	Nature and purpose of the Processing	AI involvement
All Products – technical support	End customers and users of the Data Controller whose Personal Data is stored on the Data Controller's servers.	Any Personal Data stored on the Data Controller's servers. The possibility that such data contains Personal Data of EU data subjects cannot be excluded.	Provision of requested technical support services via remote login to the Data Controller's servers. Processing is limited to possible visibility only, unless the requested services involve direct access and actual Processing on the Data Controller's instructions. In such cases, Processing may involve copying, transferring and adding data from a former system to a new system, or other professional services requested by the Data Controller. Data is stored or transferred only to destination servers specified by the Data Controller and is not retained on the Data Processor's systems unless specifically requested. Access is limited to the timeframe during which a support engineer is remotely logged into a Data Controller server.	Support tooling may include an AI support chatbot (Ada Support, Exhibit 3).
Plesk, cPanel, WHMCS (licensed on-premise / standalone)	Not applicable.	Not applicable.	No Processing of Personal Data on behalf of the Data Controller arises from the products themselves. These products are licensed to, and operated by, the Data Controller in its own environment. The Sub-Processors listed against CP, PL and WHMCS in Exhibit 3 support the Data Processor's own business operations (such as CRM, billing, support ticketing and collaboration) and do not Process Personal Data on behalf of the Data Controller. Technical support for these products is covered by the "All Products" row above.	Not applicable.
Sitejet	The Data Controller's customers, users and visitors of websites; in ecommerce use, the Data Controller's customers.	Names, email addresses and IP addresses. In ecommerce use additionally physical addresses and phone numbers.	On the Data Controller's instruction, storage of names, email addresses and IP addresses for authentication, service provision and user behaviour analysis. Where the Data Controller uses the software to set up and maintain an ecommerce store: collection, forwarding and Processing for authentication, service provision, initiation of ecommerce transactions and forwarding of data to ecommerce providers. Processing of ecommerce transaction data is limited to forwarding it to the respective ecommerce providers and to the Data Controller. Such data is not stored or maintained on the Data Processor's systems or servers.	LLM Sub-Processors are listed against SJ in Exhibit 3 (OpenAI, Google). Categories of Personal Data exposed to AI Processing: Website content

- Scope: This Agreement addresses on-premise and standalone products licensed to the Data Controller and the support services provided in relation to them. SaaS offerings that are governed by their own data processing terms, including but not limited to XOVI, Comet Backup, WebPros Cloud, SocialBee, Monitoring, etc. are not covered by this Exhibit. The data processing terms applicable to those services apply instead.
- For Service data, the Processing of data is limited to the timeframe of the underlying Service / subscription relationship.
- Every Data Processor employee or subcontractor is bound by a comprehensive WebPros Data Protection Policy. Where access to data is required to be granted from outside the EEA, such access is protected by the appropriate safeguards and guarantees (e.g. by DPA, EU Standard Contractual Clauses, EU-US Privacy Framework), required under the applicable Data privacy laws like GDPR or local data protection laws.

Exhibit 2

List of technical and organizational measures taken by WebPros as the Data Processor

1.1 Confidentiality guarantee

1.1.1 Access control

Measures designed to prevent unauthorized persons from gaining access to data processing equipment that processes or uses personal data.

Measures:
2FA login to all projects
Visitors only accompanied by employees
Office is subject to the exclusive use
Chip cards / transponder systems
Electric door locks
Building is purely an office building
Bell system without camera
Security locks
Key regulation with a list
Doors with knob on the outside
Monitored entrance area

1.1.2 Physical access control

Measures designed to prevent data processing systems (computers) from being used by unauthorized persons.

Measures:
General policy data protection and / or security
Anti-virus software
Anti-Virus Clients
Application of 2-factor authentication
Assignment of user profiles to IT systems
Use of VPN for remote access
Use of a software firewall
Login with username and password
Mobile Device Management
Encryption of data carriers
Encryption of notebooks / tablet
Smartphone encryption
Manage user permissions
Management of rights by a system administrator
Assignment of user rights

1.1.3 Data access control

Measures to ensure that persons authorized to use a data processing system have access only to data subject to their right of access and that personal data cannot be read, copied, altered or removed without authorization during processing, use and after storage.

Measures:
Document shredder (DIN 32757)
Differentiated authorizations (applications)
Use of program-technical authorization concepts
Logging of access to applications (when entering data)
Management of user rights by administrators

1.1.4 Separation control

Measures to ensure that data collected for different purposes can be processed separately. This can be ensured, for example, by logical and physical separation of data.

Measures:
Physical separation of systems
Control via an authorization concept

1.2 Ensuring integrity

1.2.1 Handover control

Measures to ensure that personal data cannot be read, copied, altered or removed without authorization during their electronic transmission or during their transport or storage on data carriers and that it is possible to verify and establish the points to which personal data are to be transmitted by data transmission facilities.

Measures:
Provisioning over encrypted connections such as sftp, https
Documentation of the deletion periods
Use of VPN technology
Functional responsibilities

1.2.2 Input control

Measures to ensure that it can be subsequently verified and established whether and by whom personal data have been entered, modified or removed in data processing systems.

Measures:
Clear responsibilities for the deletion of data
Traceability of data processing through individual user names
Use of access rights

1.3 Encryption

Measures that guarantee the pseudonymization of data.

Measures:
Encryption of data carriers in laptops / notebooks
Encryption of data in mobile devices

1.4 Ensuring availability, resilience and recoverability

1.4.1 Availability (of data)

Measures to ensure that personal data are protected against accidental destruction or loss - ensuring the availability of data.

Measures:
99.99% server hardware availability
Backup & recovery concept
Data backup concept available
RAID system / hard disk mirroring
SLA with hosting service provider
Uninterruptible power supply (UPS)

1.4.2 Load capacity (of the systems)

Measures to ensure that personal data are protected against accidental destruction or loss - Ensure the resilience of systems.

Measures:
Use of intrusion detection systems
Use of software firewalls
Installation of current security updates on all application servers
Internal and external vulnerability scanning is regularly conducted by authorized administrators as well as external specialists to help detect and resolve potential system security exposures. Anti-virus detection systems are in place throughout all servers, client devices and offices.

1.4.3 Recoverability (of data / systems)

Measures to ensure that personal data are protected against accidental destruction or loss - Ensure the recoverability of data and systems.

Measures:
Backup data intended for off - site storage is encrypted prior to transport. Client sensitive personal data is handled as Confidential Information. Daily backup of systems, storing customer personal data.
Restore databases and file systems from the web server backup

1.5 Procedures for periodic review, evaluation and evaluation

1.5.1 Order control

Measures to ensure that personal data processed on behalf of the customer can only be processed in accordance with the instructions of the customer.

Measures:
Conclusion of the necessary order data agreements
Conclusion of the necessary standard contractual clauses
Regulation on the use of subcontractors
Review of the level of protection of the contractor (initial)
Agreement on effective control rights vis-à-vis the contractor
Obligation of the contractor's employees to maintain data secrecy

1.5.2 Privacy management

Measures that ensure that methods have been evaluated to systematically plan, organize, manage and control the legal and operational requirements of data protection.

Measures:
Safety concept documented elsewhere
Appointment of an external data protection officer
Documentation of all data protection procedures and regulations
Carrying out data protection impact assessments (if required)
Compliance with the information requirements according to Art. 13 DSGVO
Use of software solutions for data protection management
Evaluate a formalized process for handling requests for information.
Implementation of suggestions for improvement
Regular sensitization of employees to data protection
Employee training on data protection
Obligation of employees to data secrecy
Access options for employees to the regulations on data protection (Wiki / Intranet)

1.5.3 Incident response management

Measures to ensure that security incidents can be prevented or, in the case of security incidents that have already occurred, that data and systems can be protected and that a rapid analysis and resolution of the security incident can be carried out.

Measures:
Documentation of security incidents
Involvement of data protection officers in security incidents
Documented process for reporting security incidents
Use of firewall and its regular updating
Use of spam filters and their regular updating
Use of virus scanners and their regular updating
Clear process for regulating responsibilities in the event of security incidents

1.5.4 Privacy friendly presets

Measures that ensure that a certain level of data protection already exists in advance through the corresponding technology design (privacy by design) and factory settings (privacy by default) of a software.

Measures:

Ensuring easy exercise of the right of withdrawal of a data subject

Personal data is only collected for the purpose for which it is required

Exhibit 3

List of Webpros Sub-Processors per product / entity

Name of Subcontractor	Location / Location of Processing	Service Type and utilizing entities/ products	Safeguards (Art. 46 GDPR)
Other Webpros Entities potentially involved in processing			
Canada Webpros International, Ltd.	2210&2209 at 4950 Yonge St., Suite 2200, Toronto, Ontario M2N 6K1 / Canada	Sales, Marketing and Support services for the WebPros Group	Adequacy Decision, DPA
Comet Licensing Ltd.	1/52 Acheron Drive, Upper Riccarton, Christchurch 8041 / New Zealand	Sales, Marketing and Support services for the Webpros Group	Adequacy Decision, DPA
SocialBee Labs Srl.	Poet Grigore Alexandrescu Str, No 51, Ap 14, 400560, Cluj-Napoca, Romania	Sales, Marketing and Support services for the Webpros Group	EU, DPA
WebPros Bulgaria EOOD	4 Marko Balabanov Street, Vazrazhdane Region, Sofia, Bulgaria	Development and Support services for the Plesk Group	EU, DPA
Webpros Germany GmbH	Hohenzollernring 72, 50672 Cologne / Germany	Sales, Marketing and Support services for the WebPros Group	EU, DPA
WebPros International GmbH	Vordergasse 59, 8200 Schaffhausen, Switzerland	Sales, Marketing and Support services for the Webpros Group	Swiss, DPA
WebPros International LLC	1100 W 23rd St, Houston, TX 77008, United States of America	Sales, Marketing and Support services for the Webpros Group	Data Privacy Framework, DPA
WebPros Japan K.K.	Minami Aoyama Bldg 4F-1974, 2-11-13 Minami Aoyama, Minato-ku, Tokyo 107-0062 JAPAN	Sales, Marketing and Support services for the Webpros Group	Adequacy Decision, DPA
WebPros Spain S.L.U.	Carrer d'Aragó, 182, Àtic, 08011 Barcelona / Spain	Sales, Marketing and Support services for the Webpros Group	EU, DPA
WHMCS Ltd.	13th Floor, One Angel Court, London, EC2R 7HJ / United Kingdom	Licensing and Support services	EU, DPA
Subprocessors used per Product / Entity			
AccessiBe, Inc.	1140 BROADWAY FL 14th, New York, NY 10001	Web Accessibility Solution (CP)	Data Privacy Framework
Ada Support Inc.	46 Spadina Ave. Toronto, Ontario, M5V 2H8, Canada	AI Support Chatbot Service (CP,PL,SJ,SB,360,CB,WC)	Adequacy Decision, DPA, EUSCC
AEB SE	Sigmaringer Straße 109, 70567 Stuttgart / Germany	Export Control Screening Service (CP,PL,SJ,SB,360,XO,WC)	EU, DPA
Amazon Web Services, Inc	410 Terry Avenue North, Seattle WA 98109, USA	Environment provider (CP,PL,SJ,SB,360,CB, WC)	DPA, EUSCC
Atlassian (Confluence / Jira)	350 Bush Street Floor 13, San Francisco, CA 94104 United States	Collaboration / Project Management Tools (CP,PL,XO,SB,360,SJ,CB,WC)	Data Privacy Framework, DPA
Auth0, Inc. (Okta)	10800 NE 8th Street, Suite 600, Bellevue, WA 98004, USA	Authentication Service (CP,PL,360,WC)	Data Privacy Framework, DPA
Automattic Inc.	60 29th Street #343, San Francisco, CA 94110	WordPress Solutions, Gravatar (PL,CP,SB,WC)	Data Privacy Framework, DPA

Calendly LLC	115 East Main Street, Suite A1B, Buford, GA 30518 / USA	Customer booking system (CB)	DPA, EUSCC
Canny Inc.	831 N Tatnall St, Wilmington, Delaware 19801 / USA	Feedback System (CB)	DPA, EUSCC
Chargebee Inc.	340 South Lemon Avenue Suite 1537 Los Angeles, CA 91789, USA	Billing System (SJ)	Data Privacy Framework, DPA
Civilized Discourse Construction Kit, Inc.	8 The Green Suite #8383 Dover, Delaware 19901, USA	Community Forum (SJ)	DPA, EUSCC
Cloudflare, Inc.	101 Townsend Street, San Francisco, CA 94107, USA	Website Bot Protection (CP,PL,360,SJ,XO,CB,WC)	Data Privacy Framework, DPA
Credly, Inc. (Acclaim)	349 5th Avenue, New York, NY 10016-5019,USA	Education badges management (CP,PL)	DPA, EUSCC
Ecwid Inc.	687 S. Coast Highway 101, Suite 239, Encinitas, CA , 92024, USA	E-Commerce solution provider (CP,PL)	Data Privacy Framework, DPA
Fonticons, Inc. (Font Awesome)	307 S. Main St. Suite 202, Bentonville, AR 72712, USA	Webfonts (CP)	DPA, Data Privacy Framework
Functional Software Inc. (Sentry.io)	45 Fremont Street, 8th Floor, San Francisco, CA 94105 / USA	Application Monitoring- and Error-Tracking (PL,360)	Data Privacy Framework, DPA
G. S. S. Rocha Digital Hardware Tecnologia	Rua João Pais 8, Apto 32, Santo Amaro, São Paulo, SP 04603-039 / Brazil	Support Contractor Brazil (PL,360)	DPA, EUSCC
Gong.io, Inc.	PO Box 190250, San Francisco, CA 94119 / USA	Revenue Intelligence platform (CP,PL,SJ,SB,360, XO,CB,WC)	Data Privacy Framework, DPA, EUSCC
Google Inc.	1600 Amphitheatre Parkway, Mountain View, CA, 94043, USA	Environment and Data Analysis provider (CP,PL,SJ,SB,360, XO)	DPA, EUSCC
Greenmark IT GmbH	Leinstraße 3, 31061 Alfeld (Leine) / Germany	Domain Provider (SJ)	EU, DPA
Help Scout	PMB 78505, PO Box 55071, Boston, MA 02205, USA	Helpdesk (SJ)	DPA, EUSCC
Hetzner Online GmbH	Industriestr. 25, 91710 Gunzenhausen / Germany	Hosting Services (SJ,360)	EU, DPA
HubSpot Inc.	25 First Street, 2nd Floor, Cambridge, MA 02141, USA	CRM and Marketing Software and Services (CP,PL,SJ,360,XO,CB,WC)	DPA, EUSCC
LiveChat, Inc.	One International Place, Suite 1400, Boston, MA, USA	Chat System (CP,PL,360,WC)	DPA, EUSCC
Livestorm SAS	16 rue Cuvier, 69006 Lyon, France	Webinar Management System (CP,PL,SJ,SB,360, XO,CB,WC)	EU, DPA
MaestroQA	33 West 17th Street, Floor 4, New York, NY 10011, USA	SupportQA System (CP,PL,SJ,SB,360,CB, WC)	Data Privacy Framework, DPA
Meetgeek	Calea Vacaresti 203A, Bucharest /& Romania	Meeting Notetaker (SB)	DPA, EUSCC
Microsoft Corporation	One Microsoft Way, Redmond, WA 98052-6399, USA	Environment (Email / Office) and Online Storage provider (CP,PL,SJ,SB,360,XO,CB, WC)	Data Privacy Framework, DPA

Mixpanel, Inc.	Pier 1, Bay 2, The Embarcadero, San Francisco, CA 94111	Analytics Platform (CP,PL,WC, CB)	Data Privacy Framework, DPA
PayPal (Europe) S.à r.l. et Cie, S.C.A.	22-24 Boulevard Royal L-2449 Luxembourg	Payment Processor (SJ,CB,WC)	DPA, EUSCC
Productboard Inc.	333 Bush St., 20th Floor, San Francisco, CA / United States of America	Feature Request System (CP,PL,CB,NO)	Data Privacy Framework, DPA, EUSCC
Realtime Board Inc. (Miro)	201 Spear Street, Suite 1100, San Francisco, CA 94105/ United States of America	Collaboration Tool (PL,CP,XO,WC)	Data Privacy Framework, DPA
Salesforce, Inc.	One Market Street, Suite 300, San Francisco, CA 94105, USA	Customer Relationship Management (CP,PL,WC)	DPA, EUSCC
Slack Technologies, Inc.	500 Howard Street, San Francisco, CA 94105, USA	Internal Messaging Service (CP,PL,SB,XO,CB,WC)	Data Privacy Framework, DPA
SparkLIT Networks Inc. (AdButler)	201 - 1001 Wharf Street, Victoria, BC, Canada	Banner Advertising Provider (XO)	Adequacy Decision, DPA
Stayln, Inc. (Spinach.ai)	812B Knox Ave Nashville, TN 37204-2618 / USA	Meeting Notetaker (CP,PL,SJ,SB,360, XO,CB,WC)	DPA, EUSCC
Stripe, Inc.	354 Oyster Point Boulevard, South San Francisco, California, 94080, USA	Payment Processor (CP,PL,SJ,360)	Data Privacy Framework, DPA
Supabase, Pte. Ltd.	71 Ayer Rajah Crescent, #03-01, Singapore 139951 / Singapore	Backend Infrastructure (NO)	DPA, EUSCC
SurveyMonkey Europe UC	70 Sir John Rogerson's Quay, Dublin 2, D02 R296 / Ireland	Survey and Outreach Tool (PL, CP, CB)	DPA, EUSCC
Talkdesk Inc.	535 Mission Street, 12th Floor, San Francisco, CA, USA	Phone system (CP,PL,360)	DPA, EUSCC
TeamViewer GmbH	Jahnstraße 30, 73037 Göppingen / Germany	Remote Collaboration Tool (CP,PL)	EU, DPA
Typeform	Carrer Bac de Roda, 163, 08018 Barcelona	Contact Form engine (CP,PL,XO,WC)	EU, DPA
UKG Inc.	2250 N. Commerce Parkway, Weston, FL 33326, USA	HR System (CP,PL,XO,SB,360,SJ)	Data Privacy Framework, DPA
Usercentrics GmbH	Sendlinger Str. 7, 80331 München	Consent Management Platform (CP,PL,SJ,SB,360, XO,CB,WC)	EU, DPA
UserVoice, Inc.	234 Fayetteville St, 3rd Floor, Raleigh, NC 27601, USA	Support Helpdesk Provider (PL,360,WC)	DPA, EUSCC
Vimeo LLC	55 West 18th Street, New York, New York 10011, United States of America	Online Video Service (XO)	DPA, EUSCC
Wasabi Technologies LLC	75 Arlington Street, Suite 810, Boston, MA 02116 / USA	Storage Infrastructure Provider (CB)	DPA, EUSCC
Wildbit, LLC	2400 Market Street, Suite 235B, Philadelphia, Pennsylvania 19103, USA	Email Messaging Provider (CP)	DPA, EUSCC

Windcave Limited	Hatfield House Et. Ss 20, 52-54 Stamford Street, London SE1 9LX / UK	Payment processor (CB)	DPA, Adequacy Decision
Wistia, Inc.	120 Brookline Street Cambridge, Massachusetts, 02139, USA	Video Content Management (SJ)	Data Privacy Framework, DPA
Worldpay (UK) Limited	The Walbrook Building, 25 Walbrook, London EC4N 8AF / UK	Payment Provider (PL)	Adequacy Decision, DPA
Yasu Suporte Tecnico em Informatica LTDA	R Santos Dumont, 1559, 85900-010 Toledo / Brazil	Support Contractor Brazil (PL,360)	DPA, EUSCC
Zapier, Inc.	548 Market St. #62411, San Francisco, CA 94104-5401, USA	Automation (SJ)	Data Privacy Framework, DPA
Zendesk, Inc.	1019 Market Street, San Francisco, CA, USA	Support ticketing system (CP,PL,SJ,SB,360,CB, WC)	Data Privacy Framework, DPA
Zoom Communications Inc.	55 Almaden Boulevard, 6th Floor, San Jose, California, 95113 / USA	Customer video calls (CB)	DPA, EUSCC
AI Subprocessors used per Product			
Anthropic / Claude	Anthropic, Inc. / Anthropic, PBC, 548 Market Street, San Francisco, CA 94104, USA	LLM Provider (NO)	DPA, EUSCC
Google / Gemini / Nano Banana	Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	LLM Provider (NO, SJ)	Data Privacy Framework, DPA
OpenAI / ChatGPT	OpenAI, Inc. / OpenAI, L.L.C., 1455 3rd Street, San Francisco, CA 94158, USA	LLM Provider (CP, PL, SJ, XO, SB)	DPA, EUSCC

Utilizing Products: cPanel (CP), Plesk (PL), Sitejet (SJ), XOVI (XO), SocialBee (SB), 360 Monitoring (360), Comet Backup (CB), WebPros Cloud (WC), Nova (NO)

The most recent list of WebPros sub-processors can be accessed via www.webpros.com anytime.

Exhibit 4

EU Standard Contractual Clauses – incorporation and annex mapping

The Standard Contractual Clauses set out in Commission Implementing Decision (EU) 2021/914 of 4 June 2021 are incorporated into this Agreement by reference and apply to every transfer of Personal Data for which they are the appropriate transfer mechanism under §8. The EUSCC are entered into by the Parties by way of their incorporation into this Agreement and do not require separate signature.

Modules: Module Two (transfer controller to processor) applies. Where the Data Controller acts as a processor on behalf of a third-party controller, Module Three (transfer processor to processor) applies instead.

Clause 7 (docking clause): applies. Clause 9 (use of sub-processors): Option 2, general written authorization, applies; the information and objection process is the one set out in §7(3) of this Agreement. Clause 11 (redress): the optional independent dispute resolution paragraph does not apply. Clause 17 (governing law): the law of the Federal Republic of Germany. Clause 18(b) (choice of forum): the courts of Germany. Clause 18(c) is unaffected, so a Data Subject may also bring proceedings in the Member State of his or her habitual residence. This choice applies to the EUSCC only and does not affect §12(3) of this Agreement.

Annex I.A (list of parties): the Parties as identified in the preamble to this Agreement. The Data Controller is identified by the account and contract data recorded for it under the Base Agreement. The Data Controller is the data exporter and the Data Processor is the data importer. Annex I.B (description of the transfer): Exhibit 1. Annex I.C (competent supervisory authority): determined in accordance with Clause 13. Annex II (technical and organizational measures): Exhibit 2. Annex III (list of sub-processors): Exhibit 3.

Swiss addendum: for transfers subject to the Swiss Federal Act on Data Protection, references to the GDPR are to be read as references to the FADP, references to EU Member States include Switzerland, the competent supervisory authority is the Federal Data Protection and Information Commissioner, and the Clauses also protect the data of legal entities until any contrary provision of Swiss law enters into force.

UK addendum: for transfers subject to United Kingdom data protection law, the International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, version B1.0, applies. Tables 1 to 3 are completed by reference to Annexes I to III above; under Table 4, the importer may end the Addendum when the Approved Addendum changes.

Exhibit 5

United States State Privacy Laws Addendum

This Exhibit applies where and to the extent the Data Processor Processes Personal Data on behalf of the Data Controller that is subject to a United States state privacy law, including the California Consumer Privacy Act as amended by the California Privacy Rights Act (the "CCPA"), the Virginia Consumer Data Protection Act, the Colorado Privacy Act, the Connecticut Data Privacy Act and the Texas Data Privacy and Security Act (together, the "US State Privacy Laws"). Terms used in this Exhibit and not defined in this Agreement have the meanings given to them in the applicable US State Privacy Law.

1. Role of the Parties. For the purposes of the US State Privacy Laws the Data Controller is the business or controller and the Data Processor is the service provider or processor. The Data Processor Processes Personal Data solely for the limited and specified purposes described in Exhibit 1 and on the Data Controller's Instructions.

2. Restrictions. The Data Processor will not: (a) sell or share Personal Data; (b) retain, use or disclose Personal Data for any purpose other than the business purposes specified in Exhibit 1, including for any commercial purpose of its own; (c) retain, use or disclose Personal Data outside the direct business relationship between the Parties; or (d) combine Personal Data received from or on behalf of the Data Controller with personal information received from or on behalf of any other person, or collected from its own interaction with the consumer, except where permitted by the applicable US State Privacy Law.

3. Compliance and notification. The Data Processor will comply with the obligations applicable to it as a service provider or processor under the US State Privacy Laws and will provide the same level of privacy protection as is required of the Data Controller. The Data Processor will notify the Data Controller without undue delay if it determines that it can no longer meet its obligations under the applicable US State Privacy Law.

4. Oversight and remediation. The Data Controller may take reasonable and appropriate steps to verify that the Data Processor uses Personal Data in a manner consistent with the Data Controller's obligations under the US State Privacy Laws, and to stop and remediate any unauthorized use of Personal Data. The audit and information rights in §6 of this Agreement satisfy this paragraph.

5. Sub-Processors. The Data Processor will impose on each Sub-Processor that Processes Personal Data subject to the US State Privacy Laws, by written contract, obligations that are materially equivalent to those set out in this Exhibit.

6. Consumer requests. The Data Processor will assist the Data Controller in responding to requests from consumers to know, access, correct or delete Personal Data, to opt out of the sale or sharing of Personal Data, or to limit the use of sensitive personal information, in accordance with §5 of this Agreement. The Data Processor will not respond directly to such a request except to refer the consumer to the Data Controller.

7. Deidentified data. Where the Data Processor Processes deidentified data, it will not attempt to reidentify the information, will maintain reasonable measures to prevent reidentification, and will contractually oblige any recipient of such data to the same restrictions.

8. Relationship to this Agreement. In the event of a conflict between this Exhibit and the remainder of this Agreement in respect of Personal Data subject to the US State Privacy Laws, this Exhibit prevails. Nothing in this Exhibit affects the application of the GDPR or the FADP to Personal Data subject to those laws.