WebPros Cloud General Terms and Conditions (GTC)

I. General Section

1. Introduction

The following Cloud General Terms and Conditions (GTC) govern the use and purchase of the cloud products and WebPros Cloud Services offered by WebPros. WebPros Cloud offers resellers, agencies, and companies fully managed cloud hosting solutions for the provision, management, and scaling of web-based services such as websites, applications, and specialized WebPros products (e.g., WHMCS, WP Squared), including automated management, security, and on-demand scaling.

Our goal is to provide customers with a secure, powerful, and flexible digital infrastructure while enabling seamless integration and management via central dashboards and APIs. Details on the scope of services and contractual terms and conditions can be found in Part I. General Section, the product-specific special terms and conditions (Part II. Special Section), and the respective service descriptions.

The use of WebPros Cloud Services is exclusively permitted to partners who have previously concluded a corresponding Partner Agreement with Plesk or cPanel. This contractual requirement serves to ensure compliance with the technical specifications and quality standards that are essential for the proper operation and management of the Cloud Services. Entering into such a Partner Agreement ensures that the services can be provided and used in a technically compatible manner. This agreement thus contributes significantly to ensuring smooth cooperation and maintaining the technical integrity of the services.

2. Contracting Parties

(1) Unless otherwise specified in a Partner Agreement concluded separately (in which case the named WebPros entity is the contracting party), these Cloud GTC of WebPros International GmbH, Vordergasse 59, 8200 Schaffhausen, Switzerland (hereinafter ‘WebPros’) apply to all contracts that an entrepreneur or legal entity under public law (hereinafter ‘Customer’ or “You”) concludes with WebPros for the SaaS services offered at https://www.webpros.com/webproscloud (hereinafter ‘WebPros Cloud’). The inclusion of the Customer's own terms and conditions is hereby rejected, unless otherwise agreed.

(2) WebPros is entitled to fulfill all contractual services (including billing services) and the resulting rights and obligations, in whole or in part through affiliated companies. Affiliated companies within the meaning of this clause are, in particular, subsidiaries, holding companies, sister companies, and other companies that are under uniform management or are linked by shareholdings, control agreements, or profit transfer agreements. The use of affiliated companies does not affect WebPros' obligations under the contract towards the Customer. WebPros remains fully responsible to the Customer for the contractual performance. Upon request, WebPros will inform the customer of the identity of the affiliated companies entrusted with the performance of the contract.

(3) Customers within the meaning of these GTC are exclusively entrepreneurs. An entrepreneur is a natural or legal person or a partnership with legal capacity who, when concluding a legal transaction, acts in the exercise of their commercial or independent professional activity. Therefore, WebPros may require sufficient proof of your entrepreneurial status when placing an order, for example, by providing your VAT ID number or other suitable evidence.

3. Conclusion of Contract

(1) The WebPros Cloud Services presented on the WebPros website do not constitute binding offers to conclude a contract but serve to enable the Customer to submit a binding offer.

(2) The Customer can submit the offer via its account in the WebPros licensing system or a form provided on the website. After entering their personal data and clicking the button or submitting the form, which completes the ordering process, they submit a legally binding contract offer with regard to the WebPros Cloud service described. All requested data must be provided completely and correctly. Subsequent changes must be updated immediately in the dashboard. After submitting the order form, you will receive an email. This email contains a link that you must use to confirm the order as part of the double opt-in procedure. This link is valid for 24 hours and will be deleted if not used. The email with the confirmation link does not constitute an order confirmation but serves as proof that the order was placed by the actual email owner.

(3) A conclusion of contract (offer and acceptance) and the acceptance of the Customer's offer by WebPros is strictly subject to the prerequisite that the Customer has previously executed and entered into a separate, valid "Partner Agreement". WebPros will only accept offers from companies that have a valid Partner Agreement in place. If no such Partner Agreement exists at the time of the order, Customer's offer is deemed ineffective and will not be accepted by WebPros.

(4) WebPros can accept the Customer's offer by sending an order confirmation in text form (e.g., email) or by providing the ordered WebPros Cloud service. If neither an order confirmation nor the provision of the service via the registration email is received within five working days of receipt of the offer, the offer shall be deemed rejected.

(5) Order processing and contact are usually carried out by email and via an automated system. The Customer must ensure that the email address provided for order processing is correct so that emails sent by WebPros can be received at this address. In particular, when using spam filters, the Customer must ensure that all emails sent by WebPros for order processing can be delivered.

4. Registration and Single Sign-On (SSO)

(1) Prior registration by the Customer is required to use WebPros' Cloud Services. The Customer is obliged to provide truthful, complete, and up-to-date information during the registration process and to update this information immediately in the event of subsequent changes.

(2) WebPros provides the Customer with login and authentication via a single sign-on (SSO) procedure. Access to the Cloud Services can be gained using the Customer's central login details or via authorized identity providers.

(3) The Customer is responsible for setting up, maintaining, and managing its user accounts, as well as for the security of the authentication information used in connection with registration or SSO use. The Customer shall ensure that only authorized users receive access data and treat it confidentially.

(4) The Customer shall take appropriate organizational and technical measures to prevent unauthorized access to the Cloud Services by third parties. These include in particular:

(i) regularly reviewing assigned SSO or access rights,
(ii) immediately blocking user accounts when employees leave the company or access data is lost,
(iii) complying with the security requirements described in the WebPros documentation.

5. Account and User Management

(1) After setting up an account, the Customer will receive access to a web-based dashboard. Within the dashboard, the Customer can view its own orders, booked products, and the respective contract and usage information.

(2) As a partner, the Customer uses the administration and assignment tools provided by WebPros to create and manage their own accounts and sub-accounts for end customers and assign them to the respective Customer products.

(3) The Customer is obliged to provide only correct and up-to-date information when managing accounts and users. Compliance with the applicable data protection and security regulations when creating and managing end customer accounts is the sole responsibility of the respective Customer.

(4) The Customer must inform its users comprehensively and in good time before the start of use about the contents of the contract, in particular the rights and obligations arising from these GTC. The Customer is liable for all breaches of duty by its users and other third parties who commit such breaches within the Customer's sphere of influence, unless it can prove that it is not at fault.

6. Technical Provisioning and Credentials

(1) Upon receipt of an order from the customer, WebPros will provide the service technically in the form of a unique API token. This API token includes in particular:
(i) the host name,
(ii) a unique token ID,
(iii) an associated password.

(2) The API token serves as the technical basis for access to start the respective service and replaces individual user accounts.

(3) The service is used based on the API token once it has been issued. The number of users actually accessing the service is irrelevant for the validity and scope of the credentials. Login via the API token is therefore independent of the number of users.

(4) The Customer is obliged to treat the API token and the access data it contains as confidential and to protect it from access by unauthorized third parties. Any misuse of access data is the responsibility of the Customer.

7. Services provided by WebPros

(1) WebPros grants the Customer the right to use the current version of WebPros Cloud for the contractually agreed services and for the agreed number of authorized users via the Internet using a browser. The scope of delivery and services as well as the approved operating environment are specified in the respective product description and in the user manual.

(2) WebPros guarantees the functionality and availability of the WebPros Cloud in accordance with the agreed service descriptions and service level agreements for the duration of the contractual relationship and will maintain it in a condition suitable for contractual use. The detailed regulations and scope of the respective services are set out in II. Special Section of the GTC.

(3) WebPros is entitled to provide the services by subcontracting to third parties (subcontractors). WebPros is liable for the performance of subcontractors as for its own actions.

(4) WebPros provides the customer with technical API documentation. This documentation is intended for the automated use of the services provided via API tokens. The API documentation contains, in particular, information on

(i) the available endpoints (including service ordering, configuration and provision of credentials),

(ii) the applicable authentication procedures using API tokens,
(iii) the technical framework conditions and parameters for integration into customer systems.

Access to the services is exclusively via the API tokens provided, and use is possible regardless of the number of users accessing the services. The customer is obliged to use the API documentation exclusively for the contractually agreed purposes and to comply with its specifications during implementation.

(6) WebPros may update or further develop WebPros Cloud at any time, without being obligated to do so. This may include adapting the cloud due to changes in the legal situation, technical developments, or to improve IT security. When doing so, WebPros will appropriately take into account the legitimate interests of the Customer and will inform customers in good time about any necessary updates. If a significant impairment to the Customer's legitimate interests occurs, the Customer shall be entitled to a special right of termination.

(7) WebPros is not obligated to adapt the WebPros Cloud to the individual needs or IT environment of the Customer.

(8) WebPros shall regularly maintain WebPros Cloud and inform the Customer in good time of any associated restrictions. Maintenance shall be carried out regularly outside the Customer's normal business hours, unless maintenance must be carried out at another time for compelling reasons.

(9) WebPros shall provide the Customer with storage space on its servers for the storage of data and for the purposes of using the WebPros Cloud, up to the extent booked. WebPros shall ensure the availability of the data within the scope of the use of WebPros Cloud. The Customer may increase or decrease the storage space volume as required in accordance with the conditions specified in II. Special Section of these GTC.

(10) WebPros guarantees the proper processing of data and compliance with technical and organizational measures to ensure data security in accordance with the standards and technologies used at WebPros, in particular to ensure the confidentiality and integrity of the processed data. At the Customer's request, WebPros will inform the customer in detail about the measures taken. However, WebPros does not assume any custody or safekeeping obligations with regard to the data. The Customer is responsible for ensuring that the data is adequately secured.

(11) The Customer remains the owner of the data stored on WebPros' servers and may request its return at any time.

(12) Insofar as WebPros provides services free of charge, these may be discontinued at any time after 30 days' notice, replaced by other solutions, or provided for a fee after your consent has been obtained.

(13) WebPros are entitled to expand services, adapt them to technical progress, and/or make improvements. This applies in particular if the adaptation appears necessary to prevent misuse or if Webpros is obliged to adapt services due to legal regulations.

(14) WebPros may provide the customer with access to a beta release without being obliged to do so. The use of beta release by the Customer is voluntary. Access to a beta release is granted solely for the purpose of enabling the Customer to evaluate the beta release during the period in which the beta release is made available by WebPros and/or to provide WebPros with feedback on the beta release. WebPros may suspend or terminate the Customer's access to a beta release at any time for any reason and without prior notice. Access to the beta release may be subject to additional terms and conditions, which may be

specified by WebPros in writing. WebPros does not guarantee that the beta versions are suitable for the purpose, meet the Customer's expectations or, are functional or complete, and the Customer acknowledges that the beta versions may contain features that WebPros will never release. It is the Customer's sole and own decision, whether or not to use a beta release, and all results arising from the use of a beta release are exclusively at Customer's own risk. The Customer acknowledges that beta releases may naturally contain errors and that they are unfinished products.

8. Scope of Use and Rights

(1) The selected products will not be physically transferred to the Customer.

(2) Unless expressly permitted by copyright law or contract, the Customer may not reverse engineer, disassemble, or decompile the products or have them reverse engineered, disassembled, or decompiled by third parties.

(3) The Customer receives the current version of the product. WebPros grants the Customer a simple, non-transferable, and non-exclusive right of use for the duration of the contract to use the contractually agreed Cloud Services within the scope of its business operations , subject to the continuous existence and validity of the Partner Agreement.

(4) The Customer is entitled to use the Cloud Services in B2B business for the provision of its own services to its end customers. This includes in particular:

(i) the use of the Cloud Services to provide their own services,
(ii) the administration and operation of end customer accounts via the functions provided,
(iii) the integration of the Cloud Services into its own business processes and products.

(5) The Customer is not permitted to resell the Cloud Services or parts thereof in isolation, to reproduce them without authorization, or to pass them on to third parties outside the intended B2B use.

(6) In the case of B2B use, the Customer remains fully responsible for compliance with all legal, contractual, and data protection requirements vis-à-vis its end customers. WebPros assumes no responsibility for this.

9. Individual Orders and Professional Services and Consulting Services via WebPros Cloud

(1) WebPros shall perform the individual orders agreed with the Customer in a service description for the use of the product and/or professional services and consulting services under the conditions of these GTC.

(2) WebPros shall perform all services with reasonable care and expertise and shall ensure that the standards and techniques used in the performance of the professional services are of satisfactory quality and suitable for the purpose.

(3) WebPros will only employ qualified and reliable personnel and will only use proven procedures, tools, and instruments whose suitability it is aware of, whose execution it has mastered, and which comply with the respective recognized rules of technology, with the exception of the voluntary use of a beta release by the Customer.

(4) WebPros is free to choose where to work and how to organize its working hours. However, WebPros must coordinate with the Customer's designated contact to ensure cooperation between the parties and adherence to deadlines.

(5) WebPros is the owner of the ancillary copyrights to all work results created for the Customer in accordance with Part II of these GTC. 'Work results' are all works created by WebPros within the scope of this contract, in particular documentation and configuration of new files, endpoints, and templates.

10. Support

(1) WebPros shall provide the Customer with support services for the Cloud Services used during the term of the contract. Support includes in particular:

(i) receiving and processing fault reports,
(ii) providing assistance with technical problems in connection with the Cloud Services,
(iii) providing information on the use of the contractually agreed functions.

(2) Support is generally provided during the business hours specified on the WebPros website or in the respective service description. Outside these hours, there is no entitlement to support unless this has been expressly agreed in the contract.

(3) Support requests must be submitted via the contact channels specified by WebPros Cloud.

(4) WebPros will process support requests with reasonable care and in accordance with technical capabilities. A specific outcome, a guaranteed response, or troubleshooting time shall only exist if this has been expressly agreed.

(5) The Customer is obliged to cooperate in the analysis and rectification of errors, in particular by providing relevant information, log data, or access rights, insofar as this is reasonable. The Customer is obliged to provide the following information with every error report:

(i) Date and time of the error occurrence,
(ii) A precise description of the error and the process in which the error was detected,
(iii) Information on whether the function in question has failed completely or whether the error only occurs under certain conditions or when processing specific data (if known),
(iv) Information on whether the error can be corrected or circumvented (if known).

(6) In individual cases, support services provided may be invoiced if the Customer has reported a malfunction and the reported malfunction occurred outside the area of responsibility of WebPros. This does not apply if the Customer, exercising due care, could not recognize that the malfunction did not occur within the area of responsibility of WebPros.

11. Service Levels; Troubleshooting

The provisions in Part II. Special Section, apply to service levels and troubleshooting for the respective products and services.

12. Obligations of the Customer

(1) The Customer and its users must protect and store the access data provided to them in accordance with the state of the art against access by third parties. The Customer shall ensure that use is only made to the extent contractually agreed. WebPros must be notified immediately of any unauthorized access.

(2) The Customer is obliged not to store any data on the storage space provided whose use violates applicable law, official orders, third-party rights, or agreements with third parties. WebPros is entitled to temporarily interrupt the connection of the server to the Internet (blocking of the WebPros Cloud) if WebPros becomes aware that posted content is illegal or there is sufficient suspicion of illegality. Sufficient suspicion of illegality exists in particular if WebPros receives a warning from the alleged injured party or is otherwise sued for injunctive relief due to the illegality of the posted content and the warning or request for injunctive relief is not obviously unfounded, or if WebPros is obliged to do so due to official orders or legal regulations. As far as possible, the Customer must be consulted beforehand or notified immediately if this is not prohibited by the competent authorities. The blocking must be limited to the potentially illegal content, as far as this is technically possible and reasonable.

(3) The current version of the Acceptable Use Policy can be viewed at https://www.webpros.com/legal. The Acceptable Use Policy is an integral part of these GTC and is binding for the Customer and every user.

(4) The Customer shall check the data for viruses or other harmful components before storing or using it in WebPros Cloud and shall use state-of-the-art measures (e.g., virus protection programs) for this purpose.

(5) The Customer is obliged to obtain and maintain all necessary licenses, approvals, and permissions required for WebPros, its contractors, and representatives to fulfill their obligations under these GTC, including, but not limited to, the WebPros Cloud Services.

(6) The Customer is responsible for regularly performing appropriate data backups and is responsible for the accuracy and recording of their user data in the Cloud Service. In accordance with Section 8, the Customer grants WebPros a non-exclusive right to use and process the user data for the provision and support of the Cloud Service and within the scope of the agreement. This includes, in particular, the creation of backups and the performance of penetration tests.

(7) When integrating third-party websites, the Customer is obligated to ensure that these do not violate applicable law. In the event of a contract being concluded with third-party providers, this shall be concluded exclusively between the Customer and the third-party provider.

(8) The Customer shall promote the use of the WebPros Cloud, the provision of services, and the creation of corresponding documents by WebPros through appropriate cooperation. In particular, the Customer shall create all technical prerequisites, provide information, and grant access necessary for WebPros to provide its services.

(9) If the Customer fails to fulfill its obligations to cooperate and WebPros is therefore unable to provide its services in whole or in part within the agreed time, the agreed period for the provision of WebPros' service shall be extended appropriately. If the Customer fails to fulfill its obligations to cooperate, WebPros shall be released from its performance obligations for this period,

insofar as the respective service cannot be provided or can only be provided with disproportionate effort due to the non-fulfillment or insufficient fulfillment of the obligations to cooperate.

13. Foreign Trade Regulations

(1) The parties agree that the services provided under this agreement may be subject to the applicable provisions of German and Swiss foreign trade laws, European foreign trade regulations, and US export regulations. Each party undertakes to comply with the export regulations relevant to its area of responsibility and to obtain the necessary approvals on its own responsibility and in a timely manner.

(2) Subject to I. General Section of these GTC, WebPros shall not be liable for any damages or other claims arising from the failure or late granting of the necessary approvals by the competent foreign trade authorities. In the event that approvals are not granted, WebPros shall not be obliged to perform its services. If approvals are granted late, contractually agreed deadlines and milestones shall be extended by the period of the delay to a reasonable extent.

(3) Upon request, the parties are obliged to immediately provide the other party with all documents and information necessary to obtain the approvals required under foreign trade law.

14. Defects Liability

(1) With regard to the provision of WebPros Cloud, the provision of storage space, and the agreement of individual orders for the use of WebPros Cloud, the defect liability provisions of rental law (Sections 253 et seq. of the Swiss OR shall apply. The customer must notify WebPros of any defects without delay. A defect does not exist in the case of malfunctions that are attributable to interference with the technical systems of WebPros for which WebPros is not responsible or to improper use of the service by the Customer. The defect liability for only insignificant reductions in the suitability of the service is excluded. Strict liability pursuant to Section 256 OR for defects that already existed at the time of conclusion of the contract is excluded.

(2) With regard to the provision of services, the warranty provisions of service law (Sections 319 et seq. OR) apply.

15. Liability

(1) WebPros shall be liable without limitation

(i) in cases of intent or gross negligence,
(ii) for injury to life, limb, or health,
(iii) in accordance with the provisions of the Product Liability Act, and
(iv) to the extent of a guarantee assumed by WebPros.

In the event of a slightly negligent breach of an obligation that is essential for achieving the purpose of the contract (cardinal obligation), WebPros' liability shall be limited to the amount of damage that is foreseeable and typical for the type of business.

(2) WebPros shall not be liable to any further extent. Unless otherwise agreed, claims for lost profits are excluded.

(3) The above limitation of liability also applies to the personal liability of WebPros' employees, representatives, and organs.

16. Legal Defects; Indemnification

(1) The Customer warrants that the content and data stored on WebPros' servers, as well as their use and provision by WebPros, do not violate applicable law, official orders, third-party rights, or agreements with third parties. The Customer shall indemnify WebPros upon first request against all third-party claims asserted on the basis of a breach of this warranty, provided that WebPros is not responsible for these claims. In addition, the Customer shall reimburse WebPros for the reasonable costs of legal action.

(2) WebPros warrants that WebPros Cloud does not infringe any third-party rights. Upon first request, WebPros shall indemnify the Customer against all third-party claims for infringements of property rights for which it is responsible in connection with the contractual use of the services and shall reimburse the costs of reasonable legal action. This is subject to the condition that the Customer immediately informs WebPros of any third-party claims asserted against it due to the contractual use of the services and grants it all necessary powers of attorney and authorizations to defend the claims.

17. Remuneration and Payment Terms

(1) The Customer shall pay the fees to WebPros in accordance with the fees applicable at the time of conclusion of the contract. The Customer shall also pay the fees for all services rendered or to be rendered in accordance with the fees applicable at the time of conclusion of the contract. The fees and charges are payable plus the applicable sales tax.

WebPros reserves the right to amend the fees charged for the services by giving the Customer at least 30 days' written notice of the change prior to the end of the then-current service term (monthly / annual).

(2) Invoices shall be sent in text form by email.

(3) Payments shall be due upon receipt of the invoice. The Customer shall pay monthly fees independent of usage, starting on the day of operational readiness, pro rata for the rest of the month (calculated on a daily basis). Thereafter, the Customer shall pay in advance (monthly/annually, as the case may be). Usage-based fees shall be invoiced monthly in arrears. Fees for services shall be invoiced after the services have been rendered, unless set forth differently in the service order document.

(4) Payments shall be made by the Customer within 14 days of the due date (receipt), unless a different payment term has been agreed in the order form or in other individual agreements. If you wish to dispute an invoice, you must inform WebPros in writing within 7 days of receipt of the invoice, stating the exact reasons for your dispute. If WebPros accepts the dispute at its sole discretion, the corresponding amount will either be credited to the next invoice or refunded to the payment method used for the contract. If WebPros rejects the dispute, you will receive written notification of this.

(5) Insofar as WebPros provides services free of charge, WebPros may discontinue these at any time after six weeks' notice, replace them with other solutions, or provide them for a fee after obtaining the Customer's consent.

(6) The Customer may only offset WebPros' claims with undisputed or legally established claims. Statutory prohibitions on offsetting remain unaffected.

(7) If the Customer defaults on payment, WebPros may temporarily block the services specified in the Customer contract. Even in the event of a block, the Customer remains obliged to pay the usage-independent fees. WebPros may charge default interest in the event of default of payment by the customer. The interest rate for the fee claim is nine percentage points above the then current base rate of the European Central Bank.

(8) WebPros uses payment service providers for invoicing and payment processing. Furthermore, WebPros may outsource billing services to its direct affiliates of the WebPros group od companies.

(9) WebPros' claim to the agreed fee shall remain valid for the duration of any suspension or other restriction of access due to illegal content.

18. Confidentiality

(1) 'Confidential Information' is all information and documents of the other party that are either marked as confidential or are to be regarded as confidential due to the circumstances or disclosure or the type of information as such, in particular information about operational processes, techniques, source code, business relationships, and know-how, as well as all work results.

(2) The parties agree to maintain confidentiality regarding such Confidential Information. This obligation shall continue for a period of 5 years after termination of the contract.

(3) This obligation does not apply to Confidential Information that

(i) was already known to the recipient at the time of conclusion of the contract or subsequently becomes known to third parties without violating any confidentiality agreement, legal provisions, or official orders;
(ii) is publicly known at the time of conclusion of the contract or subsequently becomes publicly known, provided that this is not due to a breach of this contract;
(iii) must be disclosed due to legal obligations or by order of a court or authority. To the extent permissible and possible, the recipient obliged to disclose the information shall inform the other party in advance and give it the opportunity to take action against the disclosure.

(4) The parties shall only grant access to Confidential Information to employees or vicarious agents who are subject to professional secrecy or who have previously been imposed obligations corresponding to the confidentiality obligations of this contract. Furthermore, the parties shall only disclose the Confidential Information to those employees or vicarious agents who need to know it for the performance of this contract and shall also oblige these employees to maintain confidentiality to the extent permitted by labor law for the period after their departure.

19. Data Protection and Data Processing Agreement

(1) The parties shall comply with the applicable data protection regulations applicable to them.

(2) WebPros processes the customer's personal data when providing its services as a data processor within the meaning of Art. 4 No. 8 GDPR exclusively in accordance with the instructions of the customer (controller) and the applicable data protection regulations.

(2) The parties conclude a data processing agreement (DPA) in accordance with Art. 28 GDPR with regard to the processing of personal data, which is attached hereto as Section III. This DPA and its annexes form an integral part of the contractual relationship.

20. Contract Term, Termination

(1) This contractual relationship shall come into force upon confirmation of the order or provision of the WebPros Cloud service and shall be concluded for an indefinite period. The term of the respective Customer contract shall commence upon provision of the services to the Customer.

(2) Unless mutually agreed to the contrary in any order documentation, this contract is concluded for an indefinite period and can be terminated by either party in writing with 30 days' notice to the end of the month.

(3) Since the existence of a valid Partner Agreement is a mandatory prerequisite for the conclusion of this Cloud Services contract, the termination of the underlying Partner Agreement (regardless of the reason) shall automatically and immediately result in the extraordinary termination of the applicability of these GTC. The right of use granted to the Customer under Section 8 (3) shall expire upon the termination of the Partner Agreement.

(4) The right to terminate without notice for good cause remains unaffected. Good cause shall be deemed to exist in particular if the Customer intentionally or negligently breaches a material obligation under this contract and WebPros can no longer reasonably be expected to adhere to the contract. WebPros shall be entitled to do so in particular in the event of repeated or significant payment defaults on the part of the Customer. WebPros is also entitled to terminate the contract extraordinarily if the Customer violates its obligations and WebPros has previously issued a warning.

(5) If the contractual relationship is terminated extraordinarily by WebPros due to a culpable breach of duty by the Customer, the Customer is obliged to reimburse WebPros for the termination damages resulting from the extraordinary termination, which arise from the premature termination of the contractual relationship due to the extraordinary termination, whereby WebPros must offset any expenses saved.

(6) WebPros may terminate the contractual relationship extraordinarily if the contractual services purchased are no longer produced by a supplier or manufacturer after conclusion of the contract from a certain point in time (end of life – EoL) or if the necessary technical and maintenance support is discontinued (end of service – EoS). The prerequisite for this is that fulfillment of the contract after this point in time is no longer possible without an available replacement or successor product. As soon as the supplier or manufacturer informs WebPros of the EoL or EoS date, WebPros shall immediately notify the Customer in writing and check within two months whether the service can be provided by a replacement or successor product. No later than two months after this notification, WebPros shall inform the Customer whether the contract will be continued or terminated extraordinarily from the specified date. In the event of extraordinary termination by WebPros, the Customer may terminate the contract without notice at the end of the next calendar month.

21. Data Access and Change of Provider (Data Act)

(1) The provision of WebPros Cloud Services is subject to the provisions of Regulation (EU) 2023/2854 (Data Act). These regulations specify the rights of the customer as a user and the obligations of WebPros as a provider of data processing services with regard to data access and data portability. The provisions of the General Data Protection Regulation (GDPR) always take precedence when processing personal data.

(2) The Customer has the right to receive the associated service data generated during its use of the WebPros cloud service, provided that this data is not already accessible via the standard functions of the software.

(i) WebPros shall provide this data to the Customer free of charge upon request. The data shall be provided in a structured, commonly used, and machine-readable format that facilitates further use and interoperability.
(ii) At the express request of the Customer, WebPros shall immediately transfer the data to a third party (data recipient) designated by the Customer.
(iii) The transfer of personal data to a third party also requires a valid legal basis in accordance with Art. 6 GDPR. The Customer is responsible for compliance with data protection requirements when transferring data to third parties.

(3) WebPros actively supports the Customer in migrating its data to another data processing service or to their own IT infrastructure. WebPros takes all necessary measures to facilitate the change and avoid so-called lock-in effects.

(i) Upon termination of the contract, WebPros will enable the complete transfer of customer data without undue delay. The statutory deadlines apply in the context of the change:

- The Customer may set a notice period of no more than two months.
- The transition period for the actual technical change is a maximum of 30 calendar days (unless there is a complex exception).

(ii) Upon request, WebPros shall provide the Customer with all relevant technical documentation and information on the available export and migration procedures.

(iii) Costs of switching providers:

- Until January 12, 2027, WebPros is entitled to charge reduced switching fees, which are limited to the actual, direct costs of the technical migration.
- From January 12, 2027, WebPros will no longer charge switching fees for the technical execution of the provider switch.
- Fees for other services or contractually agreed penalties for early termination remain unaffected by this provision.

(4) WebPros shall exercise the necessary care when transferring the data but is not responsible for the successful completion of the switch. In particular, the Customer is solely responsible for performing the export, ensuring the availability of a sufficient Internet connection, configuring third-party systems, and transferring data to external infrastructures. Liability for the success of these activities is excluded in accordance with Section 15 of the General Section.

(5) Insofar as Cloud Services from WebPros include a fixed monthly transfer volume, exceeding this volume may generally result in the blocking of further data traffic until the end of the billing month. However, if a change is made with the help of support services provided by WebPros, WebPros shall ensure that no relevant data traffic is blocked during the change.

(6) A change or the mere deletion of Customer content does not automatically terminate the contract. The same applies to the expiry of the transition period.

(7) The contractually guaranteed data security provided by WebPros also applies during a change and during the transition period. The Customer is expressly advised of the risks associated with a change, in particular:

(i) interruptions in the Internet connection may result in incomplete data transfers,
(ii) the necessary storage space on the Customer's side must be guaranteed,
(iii) any technical problems with third-party infrastructures are the responsibility of the Customer.

(8) All remaining Customer content will be permanently deleted by WebPros no later than 60 days after the end of the contract.

22. Protection against Government Access

(1) WebPros will only comply with requests from authorities outside the EU if there is a valid legal basis for this in the EU or an international agreement.

(2) Inadmissible data requests from third countries will be rejected.

23. Force majeure

(1) Insofar and as long as a case of force majeure exists, WebPros is temporarily released from its performance obligations.

(2) Force majeure is an external event caused by elementary forces of nature or by the actions of third parties, which is unforeseeable according to human understanding and experience and cannot be prevented or rendered harmless by economically acceptable means, even with the utmost reasonable care expected to be taken in the circumstances, and which cannot be accepted due to its frequency.

24. Final Provisions

(1) Should individual provisions of these GTC be invalid or unenforceable, the validity of the remaining provisions shall remain unaffected. The parties shall replace such provisions with valid and enforceable provisions that come as close as possible to the meaning and economic purpose and the intention of the parties at the time of conclusion of the contract. The same applies in the event of a contractual loophole.

(2) Annexes referred to in this contract are an integral part of the contract.

(3) Swiss law shall apply to this contract, excluding the UN Convention on Contracts for the International Sale of Goods.

(4) The exclusive place of jurisdiction for disputes arising from this contract is Zürich / Switzerland.

II. Special Section

1. Special provisions for the use of WHMCS software as a cloud solution and related services

The following provisions apply in addition to Section I. General Section, for the use of the 'WHMCS' software within WebPros Cloud provided by WebPros and the associated services. In the event of any contradictions, the following provisions shall take precedence over I. General Section.

1.1. Software and Service Description

(1) WHMCS is a comprehensive automation and management platform, designed specifically for providers of web hosting, domain, and IT services. WebPros provides WHMCS as a fully managed cloud solution (software-as-a-service), with the software hosted and operated on WebPros' secure server infrastructure. The platform combines customer and contract data management, automated billing and payment processing, complete product and service management, and an integrated support system in a single application.

(2) The cloud-based WHMCS solution provides the following functions, among others:

(i) Centralized collection, maintenance, and management of customer, product, and billing data,
(ii) Automated invoicing, payment processing, and dunning, including international currencies and multilingual support,
(iii) Complete domain management (registration, transfer, renewal, administration),
(iv) Integrated ticket system for optimizing customer support and communication,
(v) Security features such as SSL support, authorization management, and two-factor authentication,
(vi) Extensive customization options (templates, themes, interfaces, modules and add-ons), and
(v) Scalability according to the licensed capacity.

1.2. Technical Requirements

(1) The provision and operation of the internet access required for the use of WHMCS, the internet connections (bandwidth, stability), and the necessary end-user equipment (PC equipment, server infrastructure, mobile devices) are not covered by this contract. The Customer is solely responsible for the provision and maintenance of these components.

(2) An existing and active WebPros Cloud login for the Customer is a prerequisite for setting up and accessing the WHMCS platform. However, and solely for the use of WHMCS within WebPros Cloud, no signedpartnership agreement between a WebPros entity and the Customer is required.

(3) A standard, up-to-date Internet browser is required to access the WHMCS web interfaces. In order to use all functions without errors, JavaScript and cookies must be enabled in the customer's browser configuration.

(4) WebPros assumes no warranty or liability in accordance with Sections 14 and 15 of the I. General Section for the functionality or accessibility of WHMCS based on defective or unfulfilled technical requirements on the part of the Customer (e.g., insufficient bandwidth or an outdated browser version).

1.3. Licensing and Sublicensing

(1) The WHMCS software is provided on the basis of a main license purchased from WebPros' affiliate WHMCS Ltd. WebPros grants the customer a non-exclusive, non-transferable sublicense to use the WHMCS software license in accordance with the agreed tariff category and the associated usage capacity (number of manageable active end customers) through WebPros Cloud.

(2) Sub-licensing is staggered according to the following categories:

(i) Starter up to 250 manageable active customers.
(ii) Plus/Professional up to 500 manageable active customers.
(iii) Business up to 1,000+ manageable active customers, depending on the tariff booked.
(iv) Further capacity levels by agreement.

An active end customer within the meaning of the license pursuant to paragraph 2 is any end consumer who has at least one active product, service, add-on, or domain that is managed or billed via the WHMCS platform.

1.4. Customer Obligations regarding Sublicensing

(1) The Customer undertakes to use the sublicense granted to them exclusively for its own business purposes and not to sublicense it to third parties. Use is exclusively via the cloud infrastructure provided by WebPros. Independent installation or transfer of the software to other systems is not permitted.

(2) The Customer is obligated to comply with the agreed usage limits (number of active customers) and to immediately upgrade to a corresponding tariff if the capacity limits are exceeded. WebPros reserves the right to restrict or interrupt the service if the license capacity is exceeded until usage in accordance with the contract is restored.

(3) The sublicense granted to the Customer entitles it exclusively to the intended use of the WHMCS software within the agreed capacity limits. Any manipulation, reverse engineering, decompilation, or other technical modification of the software is prohibited. The Customer does not receive any ownership rights to the software itself, but only a temporary right of use through the WebPros Cloud system.

(4) Upon termination of the contractual relationship, the sublicense granted to the Customer shall automatically expire. The Customer is obliged to immediately back up all data resulting from the use of WHMCS. After termination of the contract, all customer data will be treated or deleted in accordance with our data protection regulations and the statutory retention periods.

1.5. Service and Support

(1) In addition to providing the cloud-hosted WHMCS software, WebPros provides the following services:

(i) Complete system administration and maintenance of the server infrastructure
(ii) Automatic software updates and security patches
(iii) Data backup and disaster recovery measures
(iv) Technical support in accordance with the service category booked
(v) Provision and maintenance of the necessary SSL certificates
(vi) Monitoring of system availability and performance

(2) Service Levels Support:

(i) Standard Support: Each customer can report incidents in the WHMCS customer area in the "Support Center" section of the WHMCS customer area. Standard support is provided on a best-effort basis with no guarantee of response time.
(ii) Priority Support: WebPros offers paid support that is available 8 hours a day, 5 days a week, with a guaranteed response time of 1 hour during those hours. Each customer is entitled to purchase priority support via the WHMCS customer area. The prices for priority support can be found in the WHMCS customer area and are hereby incorporated into this agreement by reference.

1.6. Transfer Volume

WHMCS includes a specific transfer volume per variant (see table) per billing month, which includes all incoming and outgoing data traffic. If the transfer volume is exceeded, WebPros is entitled to block the transfer of files until the end of a billing month. Unused transfer volume expires at the end of the billing month.

Product
Starter up to 250 Active Customers
Plus/Professional up to 500 Active Customers
Business up to 1,000 Active Customers

1.7. Service Level Agreement

(1) WebPros guarantees an availability of 99.5% for WHMCS, which is to be distinguished from the accessibility of end customer websites or the WebPros Cloud platform itself, for which an availability of 99.99% is guaranteed.

(2) Announced maintenance windows are to be excluded from the availability calculation. Similarly, outages for which WebPros is not responsible shall be excluded from the availability calculation. These include, for example,

(i) Impairments due to outages and/or malfunctions of technical equipment and/or network components outside the area of responsibility of WebPros;
(ii) Outages caused by IT attacks for which WebPros is not responsible;
(iii) Failures caused by improper use of software or hardware on the part of the customer;
(iv) Failures caused by the installation of security patches from the manufacturers.

(3) Availability is calculated using the following formula:

Availability (%) = ((Total time – Downtime) : Total time) ×100

(4) After receiving a fault report from the Customer, WebPros will investigate the issue and take action depending on the type of error:

(i) In the event of serious faults that make it impossible to use WHMCS as a whole or impair a main function to such an extent that contractual use is not possible, the Customer will receive notification of the processing of the report within 2 hours. WebPros aims to resolve the issue within 12 hours. If it is foreseeable that the fault cannot be resolved within this period, WebPros will inform the Customer immediately and notify them of the expected delay.
(ii) In the case of reports of other significant malfunctions in which the main or secondary functions of WebPros Cloud are impaired but still usable, or in the case of other non-insignificant malfunctions, the Customer will receive confirmation of receipt and processing of the report within 24 hours. WebPros aims to remedy these malfunctions within 72 hours.
(iii) The resolution of minor disruptions that only slightly affect the main and secondary functions of WebPros Cloud is at the discretion of WebPros. WebPros may resolve such disruptions as part of the implementation of a new release.

2. Special conditions for the use of WP Squared (Managed Service for WordPress) as a cloud solution and related services

The following provisions apply in addition to the general terms and conditions for the use of the Managed WordPress Cloud solution (WP Squared) and the associated services. In the event of contradictions, the following special provisions shall take precedence over I. General Section.

2.1. Subject Matter of the Service and Service Description

(1) With WP Squared, WebPros provides the Customer with a cloud platform for the hosting and technical management of WordPress instances. The service includes the provision of the server infrastructure, the operating system, the database, and the automated management services for the installed WordPress software.

(2) The cloud environment provided is a fully managed infrastructure platform that includes the operation of the WP Squared software. Additional licenses (e.g., cPanel, Plesk) are not required.

(3) The entire infrastructure is protected by multi-layered DDoS mitigation strategies.

(4) SSL certificates (via Let's Encrypt) are automatically requested and provided (auto-provisioning) when creating a website or adding a domain in WP Squared. The installation of custom SSLs is also possible.

(5) The service includes automated backups via WP Squared with the option of:

(i) global storage and automatic cleanup of backups.
(ii) Time-controlled scheduling of backups for domains.
(iii) Creation of on-demand backups.
(iv) Restoration from a backup.

DNS management is entirely under Customer’s control.

(6) The migration of existing websites is carried out using the WP Squared Transfer Tool on an as-I and as-available basis. Further migrations or bulk transfers can be considered on a case-by-case basis after technical review.

(7) When creating a staging site, a temporary domain is automatically assigned to enable development and testing without configuring a live domain or DNS.

(8) The WP Squared user interface can be completely white-labeled and customized to the Customer's branding (name, logo, color scheme). WebPros operates exclusively in the background. The “WebPros” brand may only be disclosed to the end user in a non-prominent manner.

2.2. Licensing and Sublicenses

(1) WebPros grants the Customer a non-exclusive, non-transferable right to use the WP Squared platform and the associated management tools for the administration of WordPress instances for the duration of the contract.

(2) The WordPress solution / software itself is open-source software (GPLv2 license). WebPros merely provides the environment and takes over the management. The use of the WordPress software by the customer is subject to the terms of the GPL license.

(3) If WebPros provides paid plugins or themes (so-called “premium components”) for use as part of the service, this constitutes a sublicense from WebPros to the Customer. These sublicenses are intended exclusively for use within the WP Squared environment. The customer is not entitled to use these premium components outside the WP Squared platform, to extract them, or to pass them on to third parties.

2.3. Obligations of the Customer

(1) The Customer may only use the WP Squared platform for the permissible operation of websites. Use for illegal, misleading, malware-spreading, or abusive purposes is strictly prohibited.

(2) The Customer is solely responsible for all content (text, images, videos) and data of their WordPress instances, as well as for the legality of the plugins and themes used. This includes compliance with data protection law (GDPR).

(3) The Customer is obliged to keep the access data provided to them (WebPros login, SFTP or database access) secret and to protect it from access by third parties.

(3) If WebPros provides updates for plugins or themes that are not covered by automated management, the Customer is obliged to install these updates themselves in a timely manner. WebPros is not liable for security vulnerabilities resulting from updates not performed by the Customer.

2.4. Technical Requirements

(1) The provision and operation of the internet access required for the use of WP Squared, the internet connections (bandwidth, stability), and the necessary end-user equipment (PC equipment, server infrastructure, mobile devices) are not covered by this contract. The Customer is solely responsible for the provision and maintenance of these components.

(2) An existing and active WebPros Cloud login for the customer and an existing cPanel partnership agreement are prerequisites for setting up and accessing WP Squared via WebPros Cloud.

(3) A standard, up-to-date internet browser is required to access the WP Squared web interfaces. In order to use all functions without errors, JavaScript and cookies must be enabled in the Customer's browser configuration.

(4) WebPros assumes no warranty or liability in accordance with Section 15 I. General Section for the functionality or accessibility of WP Squared if this is due to inadequate or unfulfilled technical requirements on the part of the Customer (e.g., insufficient bandwidth or an outdated browser version).

2.5. Resource Options

WP Squared includes a specific set of resource options per variant per billing month, which includes all incoming and outgoing data traffic. If the transfer volume is exceeded, WebPros is entitled to block the transfer of files until the end of the billing month. Unused transfer volume expires at the end of the billing month.

2.6. Service Level Agreement

WP Squared offers two different service levels.

- WebPros guarantees 99.99% availability [S1] per month for the accessibility of websites and services to end customers, i.e., services for which end customers receive a sublicense, see 2.6.2.
- For software and services used to provide services to end customers and their administration, WebPros guarantees 99.5% availability per month, see 2.6.3.

2.6.1 Calculation of availability

(1) Announced maintenance windows are to be excluded from the availability calculation. Similarly, failures for which WebPros is not responsible shall be excluded from the availability calculation. These include, for example,

(i) Impairments caused by failures and/or malfunctions of technical equipment and/or network components outside the area of responsibility of WebPros;
(ii) Failures caused by IT attacks for which WebPros is not responsible;
(iii) Failures caused by improper use of software or hardware on the part of the Customer;
(iv) Failures caused by the installation of security patches from the manufacturers.

(2) Availability is calculated using the following formula:

Availability (%) = ((Total time – Downtime) : Total time) ×100

2.6.2 Availability of end customer websites

(1) If the agreed monthly availability of 99.99% is not met, the customer will receive a credit note as specified in the following table:

Availability	Amount of credit note
99,98 % to 99,50 %	5 % of the monthly fee
99,49 % to 99,00 %	10 % of the monthly fee
98,99 % to 98,75 %	15 % of the monthly fee
98,74 % to 98,50 %	30 % of the monthly fee
< 98,49 %	50% of the monthly fee

(2) The customer must report malfunctions immediately to support in accordance with Section 10 of the General Terms and Conditions (General Section). The prerequisite for a credit note is that

(i) malfunctions detected by the Customer are sufficiently described by the Customer and can be identified by WebPros;
(ii) detected malfunctions are reported using the malfunction report form provided;
(iii) the necessary documents for troubleshooting are made available to WebPros;
(iv) the Customer has not interfered with or modified the products; (v) the product is operated under the intended operating conditions in accordance with the documentation;
(v) a fault report is submitted within 14 days of the fault occurring and a credit note is requested. After 14 days, the claim for a credit note expires.

(3) Credit notes are only issued for services and Customer websites that are not accessible. Credit notes are offset against the invoice amount in the invoice following the date on which availability fell below the required level.

2.6.2 Availability of the Administration Function

(1) WebPros guarantees 99.5% availability for the administration functions of WP Squared.

(2) After receiving a fault report from the Customer, WebPros will investigate the issue and take action depending on the type of error:

(i) In the event of serious faults that make it impossible to use WP Squared as a whole or impair a main function to such an extent that contractual use is not possible, the Customer will receive notification of the processing of the report within 2 hours. WebPros aims to resolve the issue within 12 hours. If it is foreseeable that the malfunction cannot be resolved within this period, WebPros will inform the Customer immediately and notify them of the expected delay.
(ii) In the case of reports of other significant malfunctions in which the main or secondary functions of the WebPros Cloud are impaired but still usable, or in the case of other non-insignificant malfunctions, the Customer will receive confirmation of receipt and processing of the report within 24 hours. WebPros aims to remedy these malfunctions within 72 hours.
(iii) The resolution of minor disruptions that only slightly affect the main and secondary functions of the WebPros Cloud is at the discretion of WebPros. WebPros may resolve such disruptions as part of the implementation of a new release.

3. Special conditions for the use of WebPros Nova within WebPros Cloud

These Special Conditions apply in addition to the WebPros Cloud Terms of Service for the use of WebPros Nova ("Nova"), an AI-based prompt-driven service for the generation of source code for web applications, websites, website components and images. In the event of inconsistencies, these Special Conditions shall prevail.

3.1. Subject Matter of the Service and Service Description

(1) WebPros Nova is a cloud-based AI service operated by WebPros International GmbH, enabling Customers to generate, modify and refactor source code for web applications, websites and images by means of natural-language prompts as part of the requested services. Nova functionalities offered by WebPros are strictly limited to the aforementioned. Any use of Nova beyond these limited purposes is prohibited and unlicensed.

(2) Within WebPros Cloud, Nova is exclusively provided as an integrated online service. Customers do not receive access to the underlying infrastructure, foundation models or training data.

(3) Nova relies on certain third-party General Purpose AI (GPAI) / Large Language Models (LLMs). Depending on the specific Nova functionality, the following LLMs are currently used:

AI Image Generation	Google Gemini
Nova for WordPress	Anthropic Claude, Google Gemini, OpenAI
Web Application Generation	Anthropic Claude

The utilized LLMs may unilaterally be changed by WebPros at any given time to add, improve, expand or repair Nova functionalities.
WebPros remains the contractual service provider towards the Customer. However, any changes to or outages of the underlying LLMs may cause Nova functionalities to be temporarily or permanently unavailable. By using WebPros Nova, the Customer acknowledges and accepts such risk and will not make any claims against WebPros for any damages resulting from changes to the underlying LLMs.

(4) The use of AI systems / LLMs may result in errors, distortions, or unintended inaccuracies. WebPros therefore cannot guarantee the complete accuracy, objectivity, or impartiality of content generated by AI. The information provided should therefore be critically reviewed. The accuracy of output is tied to the accuracy of the underlying LLMs, which, depending on the type of test and the specific LLM assessed, may drop below 50%.
It is therefore in the Customer's and Users' own interest to check the plausibility of the information generated by AI Systems. This is particularly important in order to avoid damage resulting from injury to life, limb or health. The Customer shall observe this and point this out to the Users of the System.

3.2. Licensing and Rights to Generated In- and Output

(1) WebPros grants the Customer a non-exclusive, non-transferable and time-limited right to use Nova during the term of the underlying license contract.

(2) Subject to mandatory third-party rights and open-source licenses, all intellectual property rights to the generated output (if any) vest in the Customer. The Customer however acknowledges that AI-generated output may not be unique, true or correct and that similar or identical output may be generated for other customers.

(3) User prompts, entered into Nova may be stored and processed by WebPros for optional security, compliance, statistical or auditing purposes. However, entered data will not be used to train the underlying LLMs, unless otherwise specifically agreed to the contrary. In its own terms towards end-customers, Customer will make sure, end-customers will exclusively use Nova for legitimate purposes, in accordance with the WebPros Acceptable Use Policy.

3.3. Obligations of the Customer

(1) The WebPros Cloud Acceptable Use Policy applies to the use of WebPros Nova. In furtherance, the Customer shall not use Nova for generating unlawful, infringing, deceptive or malicious content or code. If WebPros finds any Nova output to be in non-compliance with the WebPros Acceptable Use Policy, WebPros reserves the right to remove output, delete websites or code, temporarily or permanently suspend access to Nova or do any other action deemed appropriate or necessary to remediate the non-compliance in its own and exclusive discretion.

(2) The Customer is solely responsible for reviewing, testing, validating and securing generated code before productive deployment.

(3) WebPros Nova is not designed to handle personal data, confidential information or trade secrets. Customer shall refrain from including these types of data in any input, unless explicitly lawfully permitted.

(4) Restriction on High-Risk Use Cases
The Customer shall not use, and shall not permit any third party to use, WebPros Nova, including any AI-based features, prompt-based functionalities, models, integrations, generated outputs, APIs or related services for any purpose that qualifies as a high-risk purpose within the meaning of Regulation (EU) 2024/1689 on Artificial Intelligence ("AI Act"), in particular pursuant to Article 6 in conjunction with Annex III of the AI Act.
WebPros Nova is offered as a service, utilizing different general-purpose, prompt-driven AI models to support software development, content generation, analysis and automation tasks in a non-regulated, low-risk business environment. WebPros Nova is not designed, trained, validated, certified or contractually intended for use as, or in connection with, high-risk AI systems under the AI Act. Any use of WebPros Nova for such high-risk purposes is strictly prohibited and excluded from the scope of this Agreement.
In accordance with the provisions of the AI Act and without limitation, the Customer shall not use WebPros Nova, its Outputs or any derived results in connection with (non-exhaustive list):

- Biometric identification or biometric categorization of natural persons, including any form of remote biometric identification or authentication;
- Employment-related decision-making, including recruitment, applicant screening, performance evaluation, promotion, termination, workforce management or task allocation affecting workers or self-employed individuals;
- Eligibility assessments for essential private or public services, including credit scoring, lending decisions, insurance underwriting, access to housing, social benefits, or educational admissions;
- Medical or healthcare-related use cases, including diagnosis, treatment decisions, clinical recommendations, triage or any application impacting patient health or safety;
- Law enforcement, border control, migration or asylum contexts, including profiling, risk assessment, predictive analysis or credibility evaluation of individuals;
- Judicial, quasi-judicial or democratic processes, including assistance in judicial decision-making, legal adjudication, or influencing electoral behavior or fundamental rights.

(5) The Customer acts as the sole deployer of WebPros Nova within the meaning of the AI Act and bears exclusive responsibility for determining the suitability, legality and regulatory classification of its specific use cases. WebPros makes no representations or warranties, express or implied, that WebPros Nova or its outputs are compliant with, or suitable for, the intended purpose. The Customer shall ensure that it is authorized to use the content transmitted to the System, whether prompts, texts, drawings, photographs, etc, for this purpose. The System shall not check the permissibility of the use of the data transmitted by the Customer.

(6) Any breach of the WebPros Cloud Terms of Service or especially these Special Terms shall constitute a material breach of the license and entitle WebPros to immediately suspend or terminate the Customer's access to WebPros Nova without liability or refund.

3.4. Technical Requirements

(1) The provision and operation of the internet access required for the use of WebPros Cloud and WebPros Nova, the internet connections (bandwidth, stability), and the necessary end-user equipment (Servers, PC equipment, server infrastructure, mobile devices) are not covered by these terms. The Customer is solely responsible for the provision and maintenance of these components.

(2) An existing and active WebPros Cloud login for the customer is a prerequisite for setting up and accessing WebPros Nova via WebPros Cloud.

(3) A standard, up-to-date internet browser is required to access WebPros Nova.

(4) WebPros assumes no warranty or liability in accordance with Section 15 I of the WebPros Cloud General Terms and Conditions for the functionality or accessibility of Nova if this is due to inadequate or unfulfilled technical requirements on the part of the Customer (e.g., insufficient bandwidth or an outdated browser version).

3.5. Indemnification

The Customer indemnifies, defends and holds harmless WebPros, its affiliated companies, and their respective directors, officers, employees and agents from and against any and all claims, demands, damages, losses, liabilities, administrative fines, regulatory penalties, costs and expenses (including reasonable legal fees) arising out of or in connection with:

- the use of WebPros Nova in violation of these terms;
- the deployment of WebPros Nova as or in connection with a high-risk AI system under the AI Act;
- any failure by the Customer to comply with applicable AI-related laws, regulations or regulatory obligations, or
- any claims by Customer or third parties for infringement of intellectual property of others or the fact that the output of WebPros Nova is erroneous, dysfunctional or not fit for a specific purpose.

3.6. EU AI Act Transparency

(1) Nova is an Artificial Intelligence system within the meaning of Regulation (EU) 2024/1689 ("EU AI Act") and is currently classified as a limited-risk AI system.

(2) In accordance with Article 50 EU AI Act, Customers acknowledge that they are interacting with an AI system.

(3) Nova produces probabilistic output which may contain inaccuracies, vulnerabilities or outdated information and does not constitute professional advice.

(4) WebPros implements reasonable technical and organizational measures aligned with applicable requirements for AI systems under the EU AI Act, including AI governance, logging and input/output monitoring.

(5) WebPros may follow applicable Codes of Practice issued by the European AI Office for General Purpose AI where relevant.

(6) The Customer remains responsible for the lawful deployment, documentation and risk assessment of any AI-generated output.

(7) WebPros does not warrant that generated output is correct, complete, secure, non-infringing or fit for a particular purpose.

(8) Liability for damages arising from the use of AI-generated output is governed exclusively by the WebPros Cloud Terms of Service.

III. WebPros Cloud GTC – Data Processing Agreement

Between the provider of the WebPros Cloud platform, **WebPros International GmbH,** Vordergasse 59, 8200 Schaffhausen / Switzerland (hereinafter be referred to as the "**Data Processor**"), and the Customer, entering into a Service relationship on basis of the underlying WebPros Cloud GTC ("**Customer**" or the "**Data Controller**") (each a "Party", collectively the "Parties" hereto).
By entering into a service relationship with the Data Processor for WebPros Cloud services which involve the Processing of personal data on your behalf, this Data Processing Agreement (the Agreement"), including all exhibits hereto are made integral parts of the underlying WebPros Cloud GTC, being the contractual basis of the commercial relationship.

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, as stipulated or established via the WebPros Cloud GTC this DPA is attached to, or any other contractual understanding between the Parties, which involves the Processing of personal data on behalf of the Data Controller (collectively 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 will come into force and effect on the first date, the Customer makes use of a WebPros Cloud service on basis of the Base Agreement (the **"Effective Date"**) and will be tied to the term of the Base Agreement, unless terminated by either Party giving the other at least 3 months prior written notice of its intention to terminate. This Agreement will terminate automatically at the termination or expiry of the Base Agreement. All Exhibits hereto place integral parts of this Data Processing Agreement upon signature hereof.

§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 exclusively 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 of the Processed data 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 **Exihibit 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 is entitled to anonymise or aggregate the data so that it is no longer possible to draw conclusions about individual data subjects, and to use it in this form for the purposes of designing, developing and optimising it in line with requirements, and for providing the service agreed under the main contract. The Parties agree that data anonymised or aggregated in the manner described above is no longer personal data within the meaning of this contract.

(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 Agreement, provided that the Data Processor informs the Data Controller in advance of the location of the data Processing and the requirements of Articles 44 - 48 GDPR are met or an exception according to Article 49 GDPR applies on the basis of the adequacy decision of the European Commission pursuant to Art. 45 GDPR. Therefore, data processing in Switzerland is permitted without additional safeguards. For data processing outside the EU/EEA/Switzerland, the provisions of Articles 44–46 GDPR apply.

§ 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. An overview of the technical and organizational measures implemented by the Data Processor will be attached to this Agreement as an Exhibit.

(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 data secrecy in accordance with Article 5(f) GDPR and have committed themselves to confidentiality. 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, without undue delay, inform the Data Controller in case of a Personal Data Breach (as defined under Article 4 (12) GDPR and will investigate and provide the Data Controller with sufficient information related to the Personal Data Breach and will ensure reasonable cooperation in order to enable Data Controller to comply with any legal obligation to report the Personal Data Breach and to inform Data Subjects and the supervisory authority within the time frame provided in the Data Protection Laws.

(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.

§ 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 and Processor will be responsible for fulfilling their duties to inform resulting from Article 33 GDPR.

(3) The Data Controller will, upon termination or expiration of the Base Agreement, and, by way of issuing an Instruction, stipulate, within a period

of time set by the Data Controller, the measures to return Personal Data on carrier media or to delete stored Personal Data.

(4) The Data Controller shall be solely responsible for the lawfulness of the Processing of the data and for safeguarding the rights of the data subjects in relation to each other. Should third parties assert claims against the Data Processor based on the Processing of data in accordance with this contract, the Data Controller shall indemnify the Data Processor against all such claims upon first request.

(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) The Data Controller shall provide the Data Processor, upon request, with the information referred to in Art. 30 (2) GDPR, insofar as it is not already available to the Data Processor.

(7) If the Data Processor is obliged to provide information to a government agency or person regarding the Processing of the Data Controller data or to otherwise cooperate with such agencies, Data Controller shall be obliged to assist Data Processor in providing such information or fulfilling such other obligations to cooperate upon first request.

(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.

§ 5 Enquiries by Data Subjects or Supervisory Authorities

The Data Processor will, without undue delay, inform the Data Controller in case of any request, claim or notice from a Data Subject or any third party and assist and cooperate with Data Controller in order ensure compliance with the Data Protection Laws. Where the Data Controller, based upon GDPR or other applicable data protection law, is obliged to provide information to an individual about the collection, Processing or use of its Personal Data, the Data Processor will assist the Data Controller in making this information available, provided that the Data Controller has instructed Processor in writing to do so.

§ 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 Controller will collect voluntary disclosures from the Data Processor.
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).

If any information request, audit or inspection relates to systems provided by or on the premises of Data Processor's Sub-Processors, the scope of such information request, audit and/or inspection will be as permitted under the relevant agreement in place between Data Processor and the Sub-Processor.

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.

The Data Processor will cooperate with the Controller in the sense of Art. 28 III 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 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 Controller may subscribe to the update service in order to remain informed about any changes to this list. Alternatively, 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.

If the Data Controller does not approve a newly added Sub-Processor, then without prejudice to any termination rights under the Base Agreement and subject to the applicable terms and conditions, either Party shall have the right to either terminate this Agreement, its Instruction to Process data in writing or reject a specific form of data Processing in writing towards the Data Processor in order to avoid Processing by such new Sub-Processor.

§ 8 International Data Transfers

The Data Controller acknowledges that the Data Processor's Sub-Processors may maintain data Processing operations in countries outside the EEA or in countries without an adequate level of data protection, if it is required for the fulfillment of the Data Controller's Instructions or the underlying agreement. In such case, the Data Processor warrants that such Processing outside the EEA is protected by appropriate safeguards as requested by article 46 of GDPR. Specifically, the Data Processor will only transfer of Personal Data to entities outside the EEA if such entities are bound by EU Standard Contractual Clauses adopted by the EU Commission, Binding Corporate Rules, the EU/Swiss-US Privacy Framework(s) or such other appropriate safeguard to make sure that the foreign entity will have established an adequate level of data protection within its organization by taking the appropriate technical and organizational measures in accordance to GDPR and local data protection laws in effect.

§ 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.

§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 without limitation. 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, provided that and to the maximum extent 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 to the limitations set forth in the Base Agreement. 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 under GDPR. The Data Controller and the Data Processor act as joint debtors in respect to such claims.

(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 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 made in writing and signed by either Party 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 written form.

(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)

Exhibit 1

A description of Personal Data elements and the purpose of their Processing by the Data Processor on behalf of the Data Controller. 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.

- Depending on the specific service provided to the Data Controller within WebPros Cloud by the data Processor, different Personal Data elements may be subject to Processing as follows:

  - **WP Squared** via WebPros Cloud:
    - Contact and Identification Data: Names, company names, postal addresses, email addresses, telephone numbers, customer identification numbers of Data Controller's customers and their downstream customers;
    - Website data containing Personal Data elements
    - Technical and Access Data: IP addresses, login credentials (usernames and encrypted passwords), access logs, usage statistics;
    - Communication Data: Support ticket content and history, email correspondence, chat logs, customer service interactions;
    - IP Addresses of the Data Controller's customers, users and visitors of websites for purposes of authentication, service provision as well as user behavior analysis;
    - All other Personal Data elements stored on the WebPros Cloud platform by the Data Controller or its customers.

    WP Squared is not designed to process special categories of Personal Data within the meaning of Article 9 GDPR, and the Data Controller shall refrain from including such data in any inputs.

    The Data Processor acts as a Platform as a Service (PaaS) provider to the Data Controller for the provision of managed WordPress services to the Data Controller. Accordingly, the Data Processor will store the Data Controller's customer's hosted data on its technical infrastructure on the Data Controller's behalf and for the duration of the service provision. This type of Processing is limited to providing storage resources and related technical infrastructure support to the Data Controller, so that data stored on the Data Processor's infrastructure is subject to potential visibility to the Data Processor's engineers.

    The purpose of Processing such Personal Data elements is the provision of WebPros Cloud related services by the Data Processor on the basis of the WebPros Cloud GTC (Art. 6 I b) GDPR) and the Controller's according instructions.
    The frequency of Processing is continuous, subject to the Data Controller's use of the WebPros Cloud services and limited to the term of the underlying Base Agreement.

  - **WHMCS** via WebPros Cloud:
    - Contact and Identification Data: Names, company names, postal addresses, email addresses, telephone numbers, customer identification numbers;
    - Contract and Transaction Data: Order information, product and service details, subscription data, contract terms and conditions, service usage records;
    - Payment and Financial Data: Payment method information, bank account details, credit card information (if stored), invoice data, payment history, transaction records, billing addresses;
    - Technical and Access Data: IP addresses, login credentials (usernames and encrypted passwords), access logs, usage statistics;
    - Communication Data: Support ticket content and history, email correspondence, chat logs, customer service interactions;
    - Financial Information: Any other financial records stored on the WebPros Cloud platform in connection with the provision of services.

    WHMCS is not designed to process special categories of Personal Data within the meaning of Article 9 GDPR, and the Data Controller shall refrain from including such data in any inputs.

    The Data Processor acts as a Platform as a Service (PaaS) provider to the Data Controller. Accordingly, the Data Processor will store the Data Controller's customer's subscription and payment data on its technical infrastructure on the Data Controller's behalf and for the duration of the service provision. Personal Data will be Processed to allow the Data Controller to efficiently charge its customers for any services or goods sold by the Data Controller. Personal Data is stored on the Data Processor's infrastructure.

    The purpose of Processing such Personal Data elements is the provision of WebPros Cloud related services by the Data Processor on the basis of the WebPros Cloud GTC (Art. 6 I b) GDPR) and the Controller's according instructions.
    The frequency of Processing is continuous, subject to the Data Controller's use of the WebPros Cloud services and limited to the term of the underlying Base Agreement.

  - **WebPros Nova** via WebPros Cloud:
    Depending on the specific use of WebPros Nova within WebPros Cloud by the Data Controller, the following categories of Personal Data may be processed incidentally as part of user inputs, prompts or generated outputs:

    - Identifiers and contact data (e.g. names, usernames, email addresses) entered by the Data Controller or its authorized users as part of prompts or instructions;
    - Content data contained in source code, configuration files, website content or documentation uploaded or generated using WebPros Nova, to the extent such content includes Personal Data;
    - Technical usage data and metadata, including IP addresses, timestamps, log data and system identifiers, generated in the course of accessing and operating WebPros Nova;
    - Any other Personal Data deliberately included by the Data Controller or its users in prompts, inputs or contextual materials submitted to WebPros Nova.

    WebPros Nova is not designed to process special categories of Personal Data within the meaning of Article 9 GDPR, and the Data

Controller shall refrain from including such data in any inputs.
Data entered into WebPros Nova will not be used to train underlying language models.

Nature of Processing
The Processing consists of the automated analysis of user-provided prompts and inputs, the generation of probabilistic outputs (including source code, text, images or configuration elements), and the temporary storage and technical processing of such data as required for the provision, security, operation, monitoring and improvement of WebPros Nova within WebPros Cloud.
WebPros acts as a technical platform and AI service provider and does not determine the content, purpose or legal context of the prompts or outputs generated by WebPros Nova.

Purpose of Processing
The Processing of Personal Data is carried out solely for the purpose of providing WebPros Nova as part of WebPros Cloud, including:

- enabling prompt-based generation, modification and refactoring of source code, web applications, websites and related content;
- ensuring system functionality, security, stability, logging, auditing and compliance;
- operating, maintaining and supporting WebPros Nova in accordance with the WebPros Cloud Terms of Service and the Data Controller's documented instructions.

Processing is performed on the legal basis of Article 6(1)(b) GDPR (performance of contract) in conjunction with the underlying WebPros Cloud agreement.

Role Allocation
For the purposes of the GDPR and the EU AI Act, the Data Controller acts as the sole controller and deployer of WebPros Nova in relation to its specific use cases. WebPros acts exclusively as a Data Processor and cloud-based service provider, processing Personal Data only on behalf of and under the instructions of the Data Controller. WebPros does not use Personal Data submitted to WebPros Nova to train underlying AI models, unless expressly agreed otherwise.

Duration and Frequency of the Processing
The Processing of Personal Data occurs continuously, subject to the Data Controller's use of WebPros Nova, and is limited to the term of the underlying WebPros Cloud agreement.
Personal Data is stored only for as long as technically necessary to provide the service, comply with applicable legal obligations, or fulfill security, auditing or compliance requirements, in accordance with WebPros' retention policies.

- In the course of the provision of technical support services for WebPros Cloud by the Data Processor, the Data Processor may have the general ability to access end customer data stored on servers, although the services performed do not involve any access or actual Processing of such data by the Data Processor. Processing of such Personal Data during technical support is limited to possible visibility only, unless the nature of the requested services involve direct access and actual Processing of such data by the Data Processor on basis of the Data Controller's instructions. In such cases, Processing may involve copying, transferring and adding the data between systems or any other professional services requested by the Data Controller.

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
Bell system with camera
Security locks
Key regulation with a list
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
Differentiated authorizations (applications)
Use of program-technical authorization concepts
Logging of the output of data carriers
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:
Setting database rights
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 Pseudonymization

Measures that guarantee the pseudonymization of data.

Measures:

Internal instruction to pseudonymize personal data after expiry of the deletion period

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

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

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:

Fire and smoke detection systems
Fire extinguisher in server room
No sanitary connections in or above the server room
Protective socket strips in the server room
Server room has no windows
Server room is separated from workstations
Server room monitoring (humidity)
Server room monitoring (temperature)
Server room is air conditioned
Surge protection devices

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

2. AI-specific Technical and Organizational Measures

2.1 **Organizational Measures**

2.1.1. Governance and Policies
- Established information security and data protection governance framework.
- Designated responsibilities for data protection, information security and incident response.
- Documented risk assessments covering LLM-specific risks, including prompt handling, file uploads and output generation.

2.1.2. Personnel Security
- Access to production systems restricted on a need-to-know basis.
- Mandatory confidentiality obligations for all personnel.
- Regular training on data protection, secure development and secure use of AI systems.

2.1.3. Sub-Processor Management
- External LLM providers are selected based on documented security and privacy assessments.
- Contractual safeguards ensure that LLM providers: (i) process data solely for the purpose of providing the requested LLM service; (ii) do not use customer data for general model training or improvement; and (iii) implement appropriate technical and organizational security measures.
- Maintenance of a Sub-Processor list and, where applicable, implementation of transfer safeguards for third-country processing.

2.2. **Technical Measures**

2.2.1. Data Minimization and Purpose Limitation
- Only data required for the specific AI request is transmitted to the external LLM.
- Clear separation between: system instructions, user prompts, chat history context, and uploaded file content.
- No automatic enrichment of prompts with unrelated customer data.

2.2.2. Chat History and File Attachments
- Chat history and uploaded files are stored within the Product environment to enable continuity of user interactions.
- Access to stored chat history and files is limited to the respective customer account and authorized users.
- File attachments are processed solely to generate the requested AI output and are not transmitted beyond what is technically necessary.
- Defined retention periods apply to chat history and file uploads, after which data is deleted or anonymized in accordance with contractual and legal requirements.

2.2.3. Prompt and Output Handling
- Prompt and response content is processed for the purpose of generating the requested output and is not used for training or improving external LLMs.
- Persistent storage of prompts and responses occurs only as part of the customer-visible chat history.
- Access by personnel to prompt or response content is restricted, logged and limited to support or security purposes where strictly necessary.

2.2.4. Access Control
- Role-based access control (RBAC) across all systems.
- Multi-factor authentication (MFA) for privileged access.
- Logical tenant separation between customers.

2.2.5. Encryption and Transport Security
- Encryption in transit (TLS 1.3 or higher) for all communications between: users and the Product; and the Product and external LLM providers.

2.2.6. Logging and Monitoring
- Logging of security-relevant events and system operations.
- LLM-related logs are limited to technical metadata (e.g. timestamps, model identifiers, error states).
- Prompt, response and file content is not logged beyond the stored chat history.

2.2.7. Secure Development and Incident Response
- Secure software development lifecycle (Secure SDLC) including code reviews and vulnerability management.
- Documented incident response process, including notification of personal data breaches to customers without undue delay in accordance with the DPA.

Exhibit 3

List of Webpros Sub-Processors involved in WebPros Cloud services

Name of Subcontractor	Location / Location of Processing	Service Type and utilizing entities/ products	Safeguards (Art. 46 GDPR)
Other Webpros Entities involved in Processing			
Webpros Germany GmbH	Hohenzollernring 72, 50672 Cologne / Germany	Sales, Marketing and Support services for the WebPros Group	EU, 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
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
WebPros Bulgaria EOOD	4 Marko Balabanov Street, Vazrazhdane Region, Sofia, Bulgaria	Development and Support services for the Plesk Group	EU, DPA
WebPros International LLC	2550 North Loop W., Suite 4006 Houston, TX 77092 United States of America	Sales, Marketing and Support services for the Webpros Group	Data Privacy Framework, 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
WHMCS Ltd.	13th Floor, One Angel Court, London, EC2R 7HJ, United Kingdom	Licensing and Support services	EU, DPA
Subprocessors used per Product / Entity			
Zendesk, Inc.	1019 Market Street, San Francisco, CA, USA	Support ticketing system	Data Privacy Framework, DPA
LiveChat, Inc.	One International Place, Suite 1400, Boston, MA, USA	Chat System	DPA, EUSCC
Amazon Web Services, Inc.	410 Terry Avenue North Seattle WA 98109, USA	Environment provider	DPA, EUSCC
Google Inc.	1600 Amphitheatre Parkway, Mountain View, CA, 94043, USA	Environment and Data Analysis provider	DPA, EUSCC
Microsoft Corporation	One Microsoft Way. Redmond, WA 98052-6399, USA	Environment (Email / Office) and Online Storage provider	Data Privacy Framework, DPA
HubSpot Inc.	25 First Street, 2nd Floor, Cambridge, MA 02141, USA	CRM and Marketing Software and Services	DPA, EUSCC
Typeform	Carrer Bac de Roda, 163, 08018 Barcelona	Contact Form engine	EU, DPA
AEB SE	Sigmaringer Straße 109 70567 Stuttgart / Germany	Export Control Screening Service	EU, DPA
UserVoice, Inc.	234 Fayetteville St, 3rd Floor Raleigh, NC 27601, USA	Support Helpdesk Provider	DPA, EUSCC
Slack Technologies, Inc.	500 Howard Street, San Francisco, CA 94105, USA	Internal Messaging Service	Data Privacy Framework, DPA
MaestroQA	33 West 17th Street, Floor 4, New York, NY 10011, USA	SupportQA System	Data Privacy Framework, DPA
Auth0, Inc. (Okta)	10800 NE 8th Street, Suite 600, Bellevue, WA 98004, USA	Authentication Service	Data Privacy Framework, DPA
Cloudflare, Inc.	101 Townsend Street San Francisco, CA 94107 USA	Website Bot Protection	Data Privacy Framework, DPA
Usercentrics GmbH	Sendlinger Str. 7 80331 München	Consent Management Platform	EU, DPA

Ada Support Inc.	314-371 Front St. W, Toronto, Ontario, Canada	AI Support Chatbot Service	Adequacy Decision, DPA, EUSCC
Salesforce, Inc.	One Market Street, Suite 300, San Francisco, CA 94105, USA	Customer Relationship Management	DPA, EUSCC
Mixpanel, Inc.	Mixpanel, Inc. Pier 1, Bay 2, The Embarcadero San Francisco, CA 94111	Analytics Platform	Data Privacy Framework, DPA
Atlassian (Confluence / Jira)	350 Bush Street Floor 13 San Francisco, CA 94104 United States	Collaboration / Project Management Tools	Data Privacy Framework, DPA
Automattic Inc.	60 29th Street #343 San Francisco, CA 94110	WordPress Solutions, Gravatar	Data Privacy Framework, DPA
Gong.io, Inc.	PO Box 190250, San Francisco, CA 94119 / USA	Revenue Intelligence platform	Data Privacy Framework, DPA, EUSCC
Livestorm SAS	16 rue Cuvier, 69006 Lyon, France	Webinar Management System	EU, DPA
StayIn, Inc. (Spinach.ai)	812B Knox Ave Nashville, TN 37204-2618 / USA	Meeting Notetaker	DPA, EUSCC
Supabase, Pte. Ltd.	71 Ayer Rajah Crescent #03-01 Singapore 139951 / Singapore	Backend Infrastructure (Nova)	DPA, EUSCC
AI Subprocessors used per Product			
OpenAI / ChatGPT	OpenAI, Inc. / OpenAI, L.L.C. 1455 3rd Street San Francisco, CA 94158 USA	LLM Provider (Nova)	DPA, EUSCC
Anthropic / Claude	Anthropic, Inc. / Anthropic, PBC 548 Market Street San Francisco, CA 94104 USA	LLM Provider (Nova)	DPA, EUSCC
Google / Gemini / Nano Banana	Google LLC 1600 Amphitheatre Parkway Mountain View, CA 94043 USA	LLM Provider (Nova)	Data Privacy Framework, DPA