# WebPros Privacy Policy

v.19 - Updated November 9, 2026

## 1. General Note

This Privacy Policy is aimed at worldwide users of WebPros websites and other online services (collectively the "Offerings"). To ensure a proper and secure handling of personal data handed over to us, WebPros has decided to make the principles of the EU General Data Protection Regulation (GDPR) applicable to all its global entities as a common standard in addition to local privacy laws in effect. For Europe, both the provisions of the GDPR and the provisions of the Swiss Data Protection Act (DSG) apply, and the UK General Data Protection Regulation applies in respect of WHMCS Ltd. In the USA, the applicable privacy regulations per state apply. If your locally applicable data protection law grants you a level of data protection that exceeds that of the GDPR, this stricter level will also apply in the relationship between you and WebPros. However, the level of data protection provided by the GDPR will never be undercut.

Insofar as the terms of the GDPR are used (for example "processing" or "personal data"), these are to be understood as having the same meaning in the sense of the Swiss DSG and of your local data protection laws, insofar as this is objectively possible.

The aim of this Privacy Policy is to ensure the protection of your personal data in accordance with the fundamental requirements of the GDPR and the Swiss DSG.

The provision of your personal data is generally voluntary. Where the provision of personal data is required in order to enter into or perform a contract with us, or is required by law, we will indicate this at the point of collection. If you do not provide the data required for those purposes, we may be unable to provide the requested Offering.

## 2. Scope, Covered Offerings and Controllers

This Privacy Policy applies to the websites, web shops, documentation portals, support portals, community forums, training platforms, feature request boards, developer portals, marketplaces, partner portals, account and sign-on systems and the MCP Connector for Plesk and cPanel described in section 11.5 operated by the WebPros group under the Plesk, cPanel and WHM, WHMCS, SocialBee, Comet Backup, XOVI and WebPros brands, including their respective subdomains.

The controller for the processing described in this Privacy Policy is the WebPros group entity that operates the relevant Offering, together with WebPros International GmbH, Vordergasse 59, 8200 Schaffhausen, Switzerland, as the entity to which the group has centrally assigned the fulfillment of data subject rights. In particular, and without limitation, Comet Licensing Ltd. is the operating entity for Comet Backup, WHMCS Ltd. is the operating entity for WHMCS, SocialBee LABS SRL is the operating entity for SocialBee, WebPros Germany GmbH is the operating entity for XOVI, WebPros International GmbH is the operating entity for Plesk and WebPros International L.L.C. for cPanel and WHM. Section 4 of this Privacy Policy describes the joint processing arrangements within the group. You may address any request to privacy@webpros.com and it will be routed internally to the responsible entity.

Where an Offering is provided to you by a hosting provider, reseller, managed service provider or other WebPros partner, that partner acts as an independent controller in respect of its own customer relationship with you and applies its own privacy notice. Where we process personal data contained in your customer or end user environments on behalf of such a partner or on behalf of a business customer, we act as a processor and the applicable data processing agreement governs that processing.

Our current list of sub-processors, including the WebPros brands to which each sub-processor is allocated, is published in the legal section of www.webpros.com.

# 3. Third Country Transfer

Data processing also includes disclosure by transmission to third parties and, where applicable, to so-called third countries outside the European Union ("EU") and the European Economic Area ("EEA"). Where we transfer data to countries outside the EU or the EEA, we have labeled this below. In the case of data transfer within our group of undertakings, there are generally adequacy decisions by the European Commission pursuant to Art. 45 para. 3 GDPR for the countries in which our group company is located, namely Switzerland, Japan, the United Kingdom, New Zealand and Canada. In the case of data transfer to our group company based in the USA, such company is certified under Data Privacy Framework standards, a data processing agreement is in place and there are corresponding EU standard contractual clauses. For our group company based in India, transfers are safeguarded by the EU standard contractual clauses pursuant to Art. 46 para. 2 lit. c) GDPR together with supplementary technical and organizational measures.

Where we rely on standard contractual clauses and as legally required, we have carried out and documented a transfer impact assessment and we implement supplementary measures such as encryption in transit and at rest, access restriction on a need to know basis, and a documented policy for handling government access requests.

### 3.1 Supplementary in accordance with Swiss data protection law

For subjects resident in Switzerland, and insofar as the DSG applies, we comply with the requirements of Art. 16 et seq. DSG. Personal data is only transferred abroad if the country in question has an adequate level of data protection (for example the EU Member States, the United Kingdom, Japan, Canada, New Zealand and the USA for certain areas in accordance with the Swiss-U.S. Data Privacy Framework) or appropriate safeguards are in place to protect the data, for example by concluding standard data protection clauses, contractual agreements or other suitable protective measures.

Unless an adequacy decision or appropriate safeguards are in place, data will only be transferred in exceptional cases, for example if it is necessary to fulfill a contract or if you have given your express consent.

### 3.2 Supplementary in accordance with data protection laws in the United States

WebPros complies with the EU-U.S. Data Privacy Framework (EU-U.S. DPF), the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. WebPros has certified to the U.S. Department of Commerce that it adheres to the EU-U.S. Data Privacy Framework Principles (EU-U.S. DPF Principles) with regard to the processing of personal data received from the European Union in reliance on the EU-U.S. DPF and from the United Kingdom (and Gibraltar) in reliance on the UK Extension to the EU-U.S. DPF. WebPros has further certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this Privacy Policy and the EU-U.S. DPF Principles or the Swiss-U.S. DPF Principles, these DPF Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit https://www.dataprivacyframework.gov/.

With respect to personal data received or transferred pursuant to the DPF program, WebPros International L.L.C. is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission.

Pursuant to the DPF program, EU, UK and Swiss individuals have the right to obtain our confirmation of whether we maintain personal information relating to them in the United States. Upon request, WebPros will provide you with access to the personal information that is held about you. You may also correct, amend or delete the personal information held about you. An individual who seeks access, or who seeks to correct, amend or delete inaccurate data transferred to the United States under the DPF program, should direct their query to privacy@webpros.com. We will respond to your request within 30 days of receipt or, where a request is complex or numerous, will tell you within that period when we expect to respond, respecting the applicable legal boundaries.

Before sharing your data with third parties other than our agents, or before using it for a purpose other than the one for which it was originally collected or subsequently authorized, WebPros requires your individual and informed consent, which can be obtained via the consent management platform used by WebPros. To request to limit the use and disclosure of your personal information, please submit a written request to privacy@webpros.com.

Where personal data is sensitive, we obtain your affirmative express consent before disclosing it to a third party that is not acting as our agent, or before using it for a purpose other than that for which it was originally collected or subsequently authorized by you.

Where an organization transferring personal data to us from the United Kingdom or Gibraltar identifies that data as sensitive, we treat it as sensitive data. This includes genetic data, biometric data used for unique identification, data concerning sexual orientation, and data concerning criminal offences and convictions.

In respect of personal data received from Switzerland, we additionally treat as sensitive information on ideological or trade union related views or activities, information on social security measures or benefits, and information on administrative or criminal proceedings and sanctions other than in the context of pending proceedings.

In certain situations, we may be required to disclose personal data in response to lawful requests by public authorities, including to meet national security or law enforcement requirements. Each such request is evaluated and assessed by the WebPros Legal Department prior to making a decision about any data release. WebPros will only provide requested data if it is legally obligated to do so.

Our accountability for personal data that we receive in the United States under the DPF program and subsequently transfer to a third party is described in the DPF program principles. The categories of third parties that could be involved in the transfer or processing of your data can be viewed in section 13 of this Privacy Policy. These include, without limitation, online advertising and retargeting providers, website visitor analytics providers, session and interaction analytics providers, marketing automation and customer relationship management providers, company identification and sales intent data providers, payment and subscription billing providers, support and community platform providers, and cloud infrastructure providers. Each third party which is entrusted with personal data is bound by a data processing agreement in accordance with the data protection laws in effect. In particular, we remain responsible and liable under the DPF program Principles if third party agents we engage to process personal data on our behalf do so in a manner inconsistent with the principles, unless we prove that we are not responsible for the event giving rise to the damage.

In compliance with the DPF principles, we commit to resolve complaints about your privacy and our collection or use of your personal information transferred to the United States pursuant to the DPF program. European Union, United Kingdom and Swiss individuals with DPF program inquiries or complaints should first contact us by email at privacy@webpros.com or via post at:

WebPros International, LLC

1100 W 23rd St
Suite 153
Houston TX, 77008
legal@webpros.com

We will acknowledge your complaint promptly and will respond substantively within 45 days of receipt.

With respect to personal data transferred in reliance on the DPF program in the context of the employment relationship, WebPros commits to cooperate and comply with the advice of the panel established by the EU data protection authorities, the UK Information Commissioner's Office and the Gibraltar Regulatory Authority, and the Swiss Federal Data Protection and Information Commissioner.

For personal data other than human resources data, we have further committed to refer unresolved privacy complaints under the DPF program Principles to an independent dispute resolution mechanism, BBB

National Programs. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit https://bbbprograms.org/programs/all-programs/dpf-consumers/ProcessForConsumers for more information and to file a complaint. This service is provided free of charge to you. For human resources data, please see the paragraph above concerning cooperation with the competent data protection authorities.

If your complaint cannot be resolved through the above channels, under certain conditions you may invoke binding arbitration for some residual claims not resolved by other redress mechanisms. See https://www.dataprivacyframework.gov/framework-article/ANNEX-I-introduction.

# 4. Joint Data Processing within the WebPros Group

### 4.1 Joint Data Processing

As part of our business operations and the use of our websites, we work closely within the WebPros group and jointly process certain personal data. The goal is to make our internal processes, IT systems and administration efficient and secure. This may require us to share data within the WebPros group or process it in systems that we operate jointly, including the group wide customer relationship management platform, the group wide consent management platform, the group wide analytics and marketing measurement infrastructure, and the group wide single sign-on and account systems.

The following entities belong to the WebPros group of companies:

- WebPros International GmbH, Vordergasse 59, 8200 Schaffhausen / Switzerland

- WebPros Germany GmbH, Hohenzollernring 72, 50672 Cologne / Germany

- WebPros International L.L.C., 1100 W 23rd St, Houston, TX 77008 / USA

- WebPros Spain S.L.U., Carrer d'Aragó, 182, Àtic, 08011 Barcelona / Spain

- WebPros Bulgaria EOOD, ul. "San Stefano" 22, 1504 Sofia / Bulgaria

- WebPros Japan K.K., G1 Bldg. 7F-1221, 1-3-3 Ginza, Chuo-ku, Tokyo 104-0061 / Japan

- WebPros (India) Pvt. Ltd., B 205, Bldg-42, B-Wing, Azad Nagar Sangam CHS, Andheri, Mumbai 400053, Maharashtra / India

- Canada WebPros International, Ltd., 1055 Dunsmuir Street, Suite 3000, Vancouver, BC V7X 1K8 / Canada

- SocialBee LABS SRL, Poet Grigore Alexandrescu Str, No 51, 400560, Cluj-Napoca / Romania

- Comet Licensing Ltd., 10/248 St Asaph Street, Christchurch Central, Christchurch,8011 / New Zealand

- WHMCS Ltd., c/o TMF Group, 13th Floor, One Angel Court, London, EC2R 7HJ / United Kingdom

For data subjects from the EU, this joint data processing is based on our legitimate interest in accordance with Art. 6 para. 1 lit. f) GDPR in a well functioning corporate organization and IT infrastructure.

For persons from Switzerland, processing is also based on our overriding interest in accordance with Art. 31 para. 1 DSG in order to enable secure and efficient cooperation within the WebPros group.

To ensure data protection is maintained, we have established binding agreements within the WebPros group that specify which company assumes which tasks and responsibilities, including a joint controllership arrangement pursuant to Art. 26 GDPR in respect of the group wide marketing, analytics and account systems. The essence of that arrangement is available on request. If you have any questions or wish to exercise your rights, the WebPros company you first contacted is usually your point of contact, and you may in any event exercise your rights against any of the joint controllers.

### 4.2 Contact

We have also internally assigned the fulfillment of data subject rights to WebPros International GmbH, Switzerland. You can contact the following point of contact at any time with inquiries or to exercise your data subject rights, and they will forward your request for processing internally:

WebPros International GmbH
Vordergasse 59
8200 Schaffhausen / Switzerland
Email: privacy@webpros.com

### 4.3 Contact details of the data protection officer

The data protection officer of WebPros International GmbH can be reached at privacy@webpros.com or by post at the address stated in section 4.2 marked to the attention of the Data Protection Officer.

## 5. Data Processing on our Websites and Online Services

The individual data affected by the processing described in this Privacy Policy, the processing purposes, the legal bases, the recipients and, where applicable, transfers to third countries are listed below.

### 5.1 Contacting WebPros

When you contact us, we process the data you provide to us, for example your name, your contact details (if provided), the company you state you act for, and your message, in order to handle your request. The processing is based on our contractual or pre-contractual obligations (Art. 6 para. 1 lit. b) GDPR) or because we have a legitimate interest in responding to your inquiry (Art. 6 para. 1 lit. f) GDPR). Under Swiss data protection law, we rely on our overriding interest in communicating with you and handling your request (Art. 31 para. 1 DSG). Contact and demo request forms on our websites are provided through our customer relationship management platform HubSpot, and the data submitted is stored in that platform as described in section 5.16.

### 5.2 Contact in case of Job Applications

If you send us your application, for example by email, via a contact form or via our applicant tracking system, we will process the data you provide (such as name, email address, desired location) as well as your message and application documents solely for the purpose of processing your application. Our careers portal and applicant tracking system is operated on our behalf by a human resources information system (HRIS) provider acting as our processor. Application data is hosted in the United States and the transfer is safeguarded by the EU standard contractual clauses pursuant to Art. 46 para. 2 lit. c) GDPR and, where applicable, by the provider certification under the EU-U.S. Data Privacy Framework.

For companies based in the EU, data processing is carried out on the basis of Art. 6 para. 1 lit. b) GDPR, with Sec. 26 BDSG (decision on an employment relationship) taking precedence in Germany. If further processing is required after the procedure is completed for legal prosecution, we base this on Art. 6 para. 1 lit. f) GDPR (legitimate interests).

For applications in Switzerland, Art. 328b of the Swiss Code of Obligations applies. According to this provision, data may be processed as far as it concerns suitability for the employment relationship or is necessary for the execution of the employment contract.

Your application data will be stored for the duration of the application process. After the procedure is completed, we will delete your data within 6 months, unless there are legal retention obligations, consent for longer storage (for example for an applicant pool), or unless further retention is required to protect legitimate interests, for example to defend against claims.

We do not use automated decision making or automated scoring of candidates within the meaning of Art. 22 GDPR in our recruitment process, and we do not use emotion recognition or biometric categorization tools in recruitment.

### 5.3 Contract fulfillment and data management in the context of service provision

For the establishment, execution and processing of contracts, we process the necessary data (for example name, contact details, address, email address, phone number, access data, license and subscription data) as well as all information required for fulfilling the contract.

The processing is carried out, where applicable, in accordance with Art. 6 para. 1 lit. b) and lit. c) GDPR and the corresponding provisions of the Swiss DSG for contract fulfillment and compliance with legal obligations.

If necessary for contract processing, we transmit data to third parties, for example to supervisory authorities for correspondence or to enforce your rights. Additionally, data may be shared with our affiliated companies within the scope of order processing if they are involved in service provision.

We are subject to export control, sanctions and anti money laundering obligations. We therefore screen customer, partner and beneficial owner data against applicable sanctions and denied party lists using the Compliance Screening service of AEB SE, Stuttgart, Germany, acting as our processor. The legal basis is Art. 6 para. 1 lit. c) GDPR in conjunction with the applicable export control and sanctions regulations and, where no legal obligation applies to the relevant entity, Art. 6 para. 1 lit. f) GDPR. Under Swiss law, we rely on Art. 31 para. 1 DSG. A positive screening result is always reviewed by a human before any decision is taken.

### 5.4 Ordering, Payment and Subscription Billing

When you place an order in one of our web shops or client areas, for example at store.cpanel.net, in the Plesk online store, at whmcs.com in the client area, at marketplace.whmcs.com, in app.socialbee.com or at account.cometbackup.com, we process your order data, billing and address data, tax identification data, subscription and renewal data, and the transaction reference issued by the payment provider.

Part of our online sales is processed through a reseller of record acting as merchant in its own name, in particular Cleverbridge AG for parts of the Plesk product range. In that case the reseller of record is the seller and an independent controller for the payment transaction, and it applies its own privacy notice. In all other cases, payment is processed by specialized payment service providers acting either as independent controllers or as our processors. Full payment card numbers are entered directly with the payment service provider and are not stored by WebPros. Where we operate an affiliate or partner payout, payout data may be processed by a payment provider such as PayPal or Stripe.

The legal basis is Art. 6 para. 1 lit. b) GDPR for the performance of the contract, Art. 6 para. 1 lit. c) GDPR for statutory retention, invoicing and tax obligations, and Art. 6 para. 1 lit. f) GDPR for fraud prevention and chargeback defense. Under Swiss law we rely on Art. 31 para. 1 DSG. Invoicing and accounting data is retained for the statutory retention periods, which are up to 10 years in Switzerland and in Germany.

### 5.5 Customer, Partner and Reseller Accounts and Single Sign-On

Several of our Offerings require an account. This includes, but is not limited to Plesk 360 and WebPros Platform 360, the WebPros Account single sign-on used for signup and login at Comet Backup, SocialBee, the cPanel store and license management systems, the WHMCS client area, marketplace and license verification, including its vendor wallet and deposit functions.

For these accounts we process registration data, authentication data including hashed credentials and, where enabled, second factor data, login and session metadata including IP address and device information, entitlement and license data, support entitlements, and, in the case of partner and vendor accounts, company, tax and payout data. Where the account is used across several of our brands through single sign-on, the account data is processed jointly within the WebPros group as described in section 4.

The legal basis is Art. 6 para. 1 lit. b) GDPR for providing the account and the associated services, Art. 6 para. 1 lit. f) GDPR for account security, abuse prevention and license enforcement, and Art. 6 para. 1 lit. c) GDPR where a legal obligation applies. Under Swiss law we rely on Art. 31 para. 1 DSG. Login and security logs are retained for up to 12 months unless a longer retention is required to investigate a specific security incident or to pursue or defend legal claims.

### 5.6 Support Portals, Knowledge Bases and Community Forums

Our support portals and knowledge bases, including support.plesk.com, support.cpanel.net, help.socialbee.com, support.cometbackup.com, support.webpros.com, https://www.whmcs.com/support/ and help.university.plesk.com, are operated using Zendesk. Zendesk Inc. acts as our processor and is included in our list of sub-processors. We process the data you submit in a ticket, including your name, email address, the affected environment, the technical logs and attachments you provide, and the content of the correspondence. Legacy ticketing systems remain available at tickets.cpanel.net for historical tickets. Historical tickets from the former WHMCS ticket system have been transferred to our Zendesk based support portal within the retention period stated below.

We may also provide technical support directly to customers of our authorized resellers and respond to pre-sales inquiries from prospective customers. In these cases, we act as an independent controller for the support data, irrespective of the reseller's own customer relationship with you. Submitting a support request may require you to log in with a WebPros Account as described in section 5.5.

Our community platforms include talk.plesk.com, which is operated on the XenForo forum software, the community area of support.cpanel.net, which is operated using Zendesk community functionality, and the WHMCS community forum. Please note that content you post in a community platform, including your chosen user name, your public profile, your avatar, your signature and your posts, is publicly visible and may be indexed by search engines. Please do not post personal data or confidential information in a public community platform. The forum software uses cookies and, for the prevention of automated abuse, a captcha service. Public member directories and online user lists may be available on the forum.

The legal basis for support processing is Art. 6 para. 1 lit. b) GDPR where support forms part of a contracted service or relates to a pre-contractual inquiry, Art. 6 para. 1 lit. f) GDPR for support provided to customers of our resellers and for pre-sales inquiries, based on our legitimate interest in supporting the users of our products, and Art. 6 para. 1 lit. f) GDPR for the operation, moderation and security of the support and community platforms. Publication of your community content is based on Art. 6 para. 1 lit. a) GDPR, since you decide voluntarily to publish it, and on Art. 6 para. 1 lit. f) GDPR for the continued operation of an archive of technical discussions. Under Swiss law we rely on Art. 31 para. 1 DSG. Support tickets are retained for up to 36 months after closure. Support requests from prospective customers who do not enter into a contract with us are retained for up to 12 months after closure. Community content is retained for as long as the community platform is operated, and on deletion of your account we will anonymize your posts rather than remove technical content on which other users rely, unless you require erasure of the content itself and no overriding interest opposes this.

Where our support platforms use an AI assistant to triage or answer requests, the provisions of section 9 apply in addition.

### 5.7 Training, Certification and Learning Platforms

We operate learning and certification platforms at university.plesk.com and university.cpanel.net. For these we process your registration data, your course progress, your examination results and your certification status. Please note that these platforms may display partner leaderboards and certification directories in which your name, your company and your ranking are publicly visible. Where such publication takes place, it is based on your consent pursuant to Art. 6 para. 1 lit. a) GDPR, which you may withdraw at any time by contacting privacy@webpros.com, or on the partner agreement pursuant to Art. 6 para. 1 lit. b) GDPR. Course and certification records are retained for the validity period of the certification and for a further 3 years thereafter in order to be able to evidence the certification.

### 5.8 Affiliate, Referral and Partner Programs

We operate affiliate and referral programs for several of our brands using specialized affiliate platforms acting as our processors, in particular PartnerStack for Plesk and SocialBee and FirstPromoter for WHMCS and Comet Backup. If you join an affiliate program, we process your registration and identification data, your payout data, and the referral and conversion data generated by your referral links. If you visit our websites through an affiliate link, a referral cookie or comparable identifier is set for a limited period, typically 90 days, in order to attribute a subsequent purchase to the referring affiliate.

The legal basis for the operation of the affiliate account and payout is Art. 6 para. 1 lit. b) GDPR and, for statutory retention, Art. 6 para. 1 lit. c) GDPR. The setting of the referral identifier requires your consent pursuant to Sec. 25 para. 1 TDDDG, Art. 45c FMG or the equivalent national provision implementing Directive 2002/58/EC, and the subsequent attribution analysis is based on Art. 6 para. 1 lit. f) GDPR. Under Swiss law we rely on Art. 31 para. 1 DSG.

### 5.9 Webinars, Events and Online Meetings

For webinars and online events we use a webinar platform acting as our processor, in particular Livestorm for SocialBee and Comet Backup events. For scheduling meetings and demonstrations we use the meeting scheduling functionality of our customer relationship management platform HubSpot, including on the subdomains page.plesk.com and page.cometbackup.com. We process your registration data, your attendance data, the questions you ask, and where a session is recorded and you have been informed accordingly, the recording.

The legal basis is Art. 6 para. 1 lit. b) GDPR for organizing and providing the event you registered for, Art. 6 para. 1 lit. a) GDPR for any recording that is not necessary to provide the event and for any subsequent marketing use, and Art. 6 para. 1 lit. f) GDPR for the evaluation of attendance and engagement. Under Swiss law we rely on Art. 31 para. 1 DSG. Recording of a session is always announced at the start of the session and you may choose not to activate your camera or microphone.

### 5.10 Feature Request Boards, Surveys, Reviews and On-Site Messaging

We operate public feature request and roadmap boards, including at features.plesk.com and features.cpanel.net, on a third party platform acting as our processor. Content you post there, including your name or user name and your request, is publicly visible together with the votes it receives. We also conduct customer surveys using survey platforms acting as our processors, and we operate on-site messaging, notification bar and pop-up tools on certain websites, in particular on whmcs.com and marketplace.whmcs.com.

Our websites additionally display review badges and links to independent software review platforms such as G2, Capterra, GetApp, SourceForge and Trustpilot. Where such a badge or widget is embedded and loads content from the review platform, the review platform may receive your IP address and set its own cookies. Some of these platforms, in particular G2, additionally provide a buyer intent measurement service which is described in section 6.

Participation in surveys and the posting of feature requests is voluntary and is based on Art. 6 para. 1 lit. a) GDPR or Art. 6 para. 1 lit. f) GDPR for the analysis of aggregated feedback. The loading of third party review widgets that set cookies or comparable identifiers is based on your consent pursuant to Art. 6 para. 1 lit. a) GDPR in conjunction with the applicable national provision implementing Directive 2002/58/EC. Under Swiss law we rely on Art. 31 para. 1 DSG.

### 5.11 Accessibility Tools

On some of our websites, in particular whmcs.com, we use a third party accessibility widget which allows you to adapt the presentation of the website, for example contrast, font size, keyboard navigation and screen reader optimization. If you activate a profile in the widget, the widget stores your selection in your browser or with the provider so that it can be applied on subsequent visits. Depending on the profile you select, this

selection may allow inferences about a disability and therefore about health data within the meaning of Art. 9 GDPR. For this reason we process such a selection only on the basis of your explicit consent pursuant to Art. 9 para. 2 lit. a) GDPR and Art. 6 para. 1 lit. a) GDPR, and Art. 6 para. 7 DSG for Switzerland. You may withdraw your consent at any time by deactivating the profile in the widget or by clearing the corresponding storage in your browser. We do not use accessibility selections for analytics, advertising, lead scoring or any of the purposes described in sections 6 and 7.

### 5.12 Search Functions on our Websites

Our websites and documentation portals provide search functions. Where a search function is provided by a third party search provider, for example a hosted documentation search service on docs.cometbackup.com, the search term you enter and technical metadata including your IP address are transmitted to that provider acting as our processor in order to return the search result. This transmission is necessary in order to deliver the function you have requested and is based on Art. 6 para. 1 lit. b) and lit. f) GDPR and, under Swiss law, on Art. 31 para. 1 DSG.

Separately, we analyze which search terms are entered on our websites in order to understand which information visitors are looking for, to identify gaps in our documentation and to improve our content. Where this analysis is carried out using an analytics service that sets or reads cookies or comparable identifiers on your device, or which enriches the search term with other analytics data relating to you, we carry out that analysis only if you have given the corresponding consent in our consent management platform. Where we evaluate search terms in a purely aggregated and non-identifying form, we rely on Art. 6 para. 1 lit. f) GDPR and Art. 31 para. 1 DSG. Search terms are transmitted to Google Analytics only within the scope of the consent you have given for the Analytics category.

Please do not enter personal data, credentials or confidential information into a search field. We do not use website search terms to build a profile of you by name and we do not sell search terms.

### 5.13 Embedded Third-Party Content and Media

Our websites, blogs, documentation and community platforms embed content hosted by third parties, in particular videos from YouTube and Vimeo, media from a content delivery network operated for the WebPros group, avatars from an avatar service, and social media embeds and share functions for platforms such as Facebook, Instagram, LinkedIn, X, TikTok, Reddit, Pinterest and YouTube. When such content is loaded, the third party provider receives your IP address and may set cookies or read information already stored on your device, and may combine this information with an existing account you hold with that provider.

For this reason, embedded third party content that is not strictly necessary is loaded only after you have given your consent in our consent management platform. The legal basis is Art. 6 para. 1 lit. a) GDPR in conjunction with the applicable national provision implementing Directive 2002/58/EC, and Art. 6 para. 6 DSG for Switzerland. We have no influence on the further processing carried out by the third party provider in its own responsibility. Please consult the privacy notice of the relevant provider for further information.

### 5.14 Log Files of Website Visits

We log your website visit. In doing so, we process:

- The name or names of our accessed websites
- The date and time of access
- The amount of data transferred
- The browser type and version
- The operating system you use
- The referrer URL, meaning the previously visited website

- Your IP address

- The requesting provider

- The HTTP status code and the requested resource

The legal basis for this data processing is our overriding legitimate interest in the continuous provision, stability and security of our websites in accordance with Art. 6 para. 1 lit. f) GDPR and Art. 31 para. 1 DSG. Server log files are deleted after seven days unless they are needed to prove or clarify specific legal violations that have become known within the retention period. Security and abuse logs generated by our content delivery and bot protection providers may be retained for a longer period as described in section 5.15.

Server log data is used for the operation and security of the websites. It is not used for the analytics, company identification, buying intent or advertising purposes described in sections 6 and 7.

### 5.15 Content Delivery, Performance Optimization and Bot Protection

We use content delivery network, web application firewall, bot management and performance optimization services in order to deliver our websites reliably and to protect them against denial of service attacks, credential stuffing, scraping and other abuse. These services necessarily process your IP address, request metadata and technical fingerprint information, and they set strictly necessary cookies. Where a caching or performance optimization service is used on a website, it may set its own cookies in order to serve the correct cached version of a page to you.

On forms, registration pages and login pages we use captcha and bot verification services, in particular Google reCAPTCHA on socialbee.io, whmcs.com and cometbackup.com and a captcha service on talk.plesk.com. These services process your IP address, your interaction with the page and technical browser and device information in order to distinguish human users from automated requests.

The legal basis is Art. 6 para. 1 lit. f) GDPR and Art. 31 para. 1 DSG, based on our legitimate interest in the availability and security of our websites and in the prevention of abuse and fraud, and Art. 6 para. 1 lit. c) GDPR insofar as we are required to implement appropriate security measures pursuant to Art. 32 GDPR. Where a captcha or performance service is not strictly necessary for the requested function, it is loaded only after consent. Security log data is retained for up to 12 months, and longer only where required to investigate a specific incident or to pursue or defend legal claims.

### 5.16 Newsletter, Customer Information and Marketing Communication

To keep you regularly informed about our company and our offers, we operate several email newsletters. For this purpose we process the data you provide during registration, namely your email address and any voluntary information such as your name, your company and your role.

To prevent misuse, we use the double opt-in procedure. After registration you confirm it through a confirmation email. The registration process is logged in order to prove its legality, namely the time of registration and confirmation as well as the IP address. The legal basis is your consent, for the EU pursuant to Art. 6 para. 1 lit. a) GDPR and for Switzerland pursuant to Art. 31 para. 1 DSG. The logging and the confirmation email are based on our legitimate interest in proving proper registration pursuant to Art. 6 para. 1 lit. f) GDPR and Art. 31 para. 1 DSG.

Our newsletters and marketing emails contain measurement technologies, in particular tracking pixels and individualized links, which allow us to determine whether and when an email was opened, which links were clicked, and which pages of our websites you visited afterwards. This measurement is carried out at the level of the individual recipient and is combined with the other data held about you in our customer relationship management platform, including for the purposes described in section 6. The legal basis for this measurement is your consent pursuant to Art. 6 para. 1 lit. a) GDPR, which is obtained together with the newsletter registration. You may withdraw this consent at any time with effect for the future, either by

unsubscribing from the newsletter or by contacting privacy@webpros.com, and you may prevent the measurement by configuring your email client not to load external images.

The data is transmitted to HubSpot, Inc. (USA) as part of order processing. HubSpot is certified under the EU-U.S. and Swiss-U.S. Data Privacy Framework, ensuring an adequate level of data protection under both EU and Swiss law. Additionally, EU standard contractual clauses are in place. European branch: HubSpot Ireland Ltd., 30 North Wall Quay, Dublin 1, Ireland.

Based on our legitimate interest in accordance with Art. 6 para. 1 lit. f) GDPR and the existing customer relationship with WebPros, customers may be provided with information relating to other WebPros products which may be of interest to them. Where a WebPros entity established in Germany sends such information, it does so only in respect of its own similar goods or services, only to a customer from whom the email address was obtained in connection with the sale of a good or service, only where the customer has not objected, and only where the customer was clearly informed at the time of collection and in each communication that they may object at any time, in accordance with Sec. 7 para. 3 of the German Act against Unfair Competition. At any time, customers have the option to opt out of the receipt of such information by using the unsubscribe option in any communication received or by contacting privacy@webpros.com.

Newsletter registration and consent records are retained for the duration of the subscription and for a further 3 years after withdrawal in order to be able to evidence the lawfulness of the processing. Where you object to marketing, we retain a minimal suppression record for as long as necessary to give effect to your objection.

## 6. Website Analytics, Visitor Measurement and Business Intent Analysis

WebPros collects analytical data while you visit our websites and processes that analytical data for its own purposes. This section describes that processing in detail. It applies in addition to, and not instead of, the provisions on cookies and similar technologies in section 8 and the provisions on advertising in section 7.

### 6.1 Analytical data collected during your website visit

When you visit one of the Offerings listed in section 2, we collect and process analytical data about your visit. Depending on the Offering and on the consent you have given, this may include:

- Online identifiers, in particular cookie identifiers, client identifiers, session identifiers, device identifiers and comparable identifiers stored on or read from your terminal device

- Your IP address, and the network, host name, autonomous system and approximate geographic location derived from it

- Technical characteristics of your device and software, including browser type and version, operating system, language settings, screen resolution, device category and referrer

- Navigation and page view data, including the pages, documentation articles, pricing pages, product pages, download pages and blog articles you view, the order in which you view them, the time spent on each page, and your scroll depth

- Interaction data, including clicks, mouse movement, hovering, form field focus and abandonment, downloads, video plays, expansion of accordions and use of on-site search

- Entry and exit points, campaign parameters, referring search engines and referring third party websites, and the marketing campaign, advertisement or affiliate link through which you reached us

- Conversion and commercial events, including trial starts, license activations, cart views, checkout steps, purchases, demo requests, contact form submissions, webinar registrations and newsletter registrations

- Engagement with our marketing emails as described in section 5.16, where you have consented to that measurement

- Where you are logged in to one of our accounts or have identified yourself to us, for example by submitting a form, the association between the above analytical data and your account or contact record, including your name, email address, company and role

Where technically available, we link the analytical data collected across our own domains and subdomains, including across our marketing websites, documentation portals, support portals, web shops and account systems, so that a visit spanning several of these domains is measured as a single visit rather than as several unrelated visits.

### 6.2 Purposes of processing and our own use of analytical data

We process the analytical data described in section 6.1 for our own purposes and in our own responsibility as controller. The purposes are:

- Measuring reach, audience and content performance, and understanding how our Offerings are found and used

- Detecting technical errors, broken navigation paths and performance problems, and improving the stability, usability and structure of our Offerings

- Improving our documentation, knowledge base articles and product information on the basis of what visitors actually look for and read

- Measuring the effectiveness of our marketing campaigns, advertisements, affiliate placements, newsletters and events, and attributing conversions to the campaigns that produced them

- Optimizing our Offerings by testing alternative versions of pages, content and functions

- Analyzing user activity in order to determine which company or organization a visit is likely to originate from, as described in section 6.3

- Analyzing user activity in order to determine signals of purchase readiness and commercial interest, as described in section 6.4

- Prioritizing and personalizing our sales and marketing activities, including deciding which prospects our sales teams contact, in which order, with which product focus and with which message

- Producing internal business reporting, market and demand analysis, pipeline forecasting and product strategy

- Detecting and preventing abuse, fraud, license misuse and automated scraping of our Offerings

Analytical data is used by us for our own purposes as described above. We do not sell analytical data. Where analytical data is disclosed to a third party, this is done either to a processor acting on our instructions, or to an advertising partner within the scope of section 7 and only on the basis of your consent.

### 6.3 Identification of the acting company

Our Offerings are directed primarily at businesses, in particular at hosting providers, managed service providers, web professionals, agencies and their staff. In order to understand which businesses are interested in our products, we evaluate the analytical data described in section 6.1 with the aim of determining the company or organization on whose behalf a visitor is acting.

For this purpose we process, in particular, your IP address and the network and host information derived from it, the company domain of an email address you have provided to us, information you have provided in a form, and the pattern of pages viewed during the visit and across visits. We compare this information against commercially available business databases and network registries, in order to associate the visit with a company, an industry, a company size, a geographic market and, where available, publicly available contact information for the relevant business function. This process is commonly referred to as reverse IP lookup, company identification, firmographic enrichment or account identification.

The result of this process is an assessment at the level of the company. However, because the assessment is derived from data relating to your individual visit, and because it may be linked to your contact record where you have identified yourself to us, this processing constitutes the processing of personal data relating to you and, where the assessment is used to evaluate your behavior and interests, it constitutes profiling within the meaning of Art. 4 no. 4 GDPR.

The identification of the acting company is not always accurate. In particular, an IP address may be assigned to an internet access provider, to a mobile network, to a shared office, to a virtual private network or to a hosting provider rather than to the company you actually work for, and business databases may contain outdated information. We therefore treat the result as an indication and not as a certainty, and no measure with a legal or similarly significant effect on you is taken on the basis of this assessment.

**6.4 Determination of buying intent signals and lead prioritization**

We further evaluate the analytical data described in section 6.1, together with the company assessment described in section 6.3 and with the data held about you and about your company in our customer relationship management platform, in order to determine signals of purchase readiness and commercial interest. This is commonly referred to as intent data, buyer intent, engagement scoring or lead scoring.

The signals we evaluate include, in particular:

- Which product, edition, extension or pricing pages were viewed, how often and how recently

- Repeat visits from the same identifier or from the same company within a given period, and any increase in the intensity of such visits

- Views of pages that typically precede a purchase decision, for example pricing, comparison, migration, licensing, reseller, enterprise and total cost of ownership pages

- Downloads of trial versions, technical documentation, white papers and comparison material

- Registrations for webinars, events and demonstrations, and attendance at them

- Engagement with our marketing emails, advertisements and affiliate placements

- Use of the on-site search function and the specific terms searched for

- Product and account signals available to us, for example trial usage, license status, expiry dates and prior purchases

- Signals made available to us by independent software review platforms in relation to research activity on our product categories, as described in section 5.10

On the basis of these signals we calculate a score or a qualitative classification for a visitor, a contact and a company. We use that score in order to decide which prospects our sales and marketing teams approach, at what time, with which product focus and with which message, and in order to plan our sales capacity and our marketing spend. We may also use it in order to select which content, offers or on-site messages are shown to you.

This processing constitutes profiling within the meaning of Art. 4 no. 4 GDPR. It does not constitute a decision based solely on automated processing which produces legal effects concerning you or similarly significantly affects you within the meaning of Art. 22 GDPR or Art. 21 DSG. No price, no product availability, no credit decision, no eligibility decision and no contractual term is determined on the basis of the score. A score is at most a prioritization for human sales activity, and any contact with you is initiated and conducted by a member of our staff.

**6.5 Interaction analytics, session recording and heatmaps**

On several of our websites we use interaction analytics services which record how visitors interact with a page. Depending on the service and the Offering, these services generate aggregated heatmaps of clicks, mouse movement and scroll depth, and they may create a reconstructed recording of an individual session,

meaning a replay of the mouse movements, clicks, scrolling, page transitions and, where enabled, non sensitive form interactions of a single visit. The services currently used for this purpose are Hotjar on plesk.com and cpanel.net and Microsoft Clarity on webpros.com, cpanel.net, socialbee.io, whmcs.com and cometbackup.com. These providers act as our processors.

We configure these services so that password fields, payment fields and fields designated as sensitive are suppressed at the point of capture and are not transmitted, and so that IP addresses are truncated or not stored where the service offers that option. Nevertheless, a session recording can be intrusive, and information that you type into a free text field may be captured. Please therefore do not enter personal data or confidential information which you do not wish us to see into free text fields on our websites.

Session recording and heatmap analytics are activated only if you have given the corresponding consent in our consent management platform. The legal basis is Art. 6 para. 1 lit. a) GDPR and Art. 6 para. 6 DSG, together with the applicable national provision implementing Directive 2002/58/EC. Recordings and heatmap data are retained for the retention period configured with the provider, which does not exceed 12 months, and are then deleted.

### 6.6 Website optimization and A/B testing

On some of our websites we use an experimentation service in order to test alternative versions of pages, headlines, forms and functions and to determine which version performs better. For this purpose the service assigns you to a test group, stores that assignment in an identifier on your device, and measures the events described in section 6.1 separately per test group. This is activated only on the basis of your consent pursuant to Art. 6 para. 1 lit. a) GDPR in conjunction with the applicable national provision implementing Directive 2002/58/EC, and Art. 6 para. 6 DSG for Switzerland. Test group assignment does not affect the price, the availability or the contractual terms of any product.

### 6.7 Legal bases for the processing described in this section

Insofar as the collection of the analytical data described in section 6.1 requires the storage of information on your terminal device or access to information already stored on your terminal device, and that storage or access is not strictly necessary in order to provide the service you have expressly requested, we carry it out only on the basis of your consent pursuant to Sec. 25 para. 1 TDDDG for Germany, Art. 45c FMG and Art. 6 para. 6 DSG for Switzerland, and the corresponding national provision implementing Directive 2002/58/EC in other jurisdictions. That consent is obtained through our consent management platform and is documented as described in section 8.2.

The subsequent processing of the analytical data, including the company identification described in section 6.3 and the buying intent analysis described in section 6.4, is based on:

- Art. 6 para. 1 lit. a) GDPR, where the processing is based on the consent you have given in our consent management platform, in particular for all processing in the Analytics and Marketing cookie categories, for session recording, for A/B testing and for the transmission of data to advertising partners

- Art. 6 para. 1 lit. f) GDPR, on the basis of our legitimate interest in understanding the market for our products, in addressing potential business customers efficiently, in allocating our sales and marketing resources sensibly, and in operating, securing and improving our Offerings, insofar as the processing does not require consent

- Art. 31 para. 1 DSG, on the basis of our overriding interest, for processing governed by Swiss law

- Art. 6 para. 1 lit. b) GDPR, where the analysis of usage data forms part of a service you have contracted for

We have carried out and documented a balancing of interests in respect of the processing based on Art. 6 para. 1 lit. f) GDPR. In that assessment we have taken into account, in particular, the business to business context of our Offerings, the fact that the assessment is aimed at the acting company rather than at your private life, the fact that no decision with a legal or similarly significant effect is taken on the basis of the

assessment, the limited retention periods, and the unconditional right to object described in section 6.10. A summary of that balancing of interests is available on request from privacy@webpros.com.

### 6.8 Recipients and third country transfers

The analytical data described in this section is processed by us and by processors acting on our instructions. These include our web analytics providers, our interaction analytics providers, our experimentation provider, our tag management provider, our customer relationship management and marketing automation provider, our company identification and business intent data providers, and our cloud infrastructure providers. Within the WebPros group the analytical data is processed jointly as described in section 4, in particular in the group wide customer relationship management platform and the group wide analytics infrastructure.

Several of these providers are established in the United States or process data in the United States. Those transfers are safeguarded by the EU-U.S. Data Privacy Framework where the provider is certified, and otherwise by the EU standard contractual clauses pursuant to Art. 46 para. 2 lit. c) GDPR together with the supplementary measures described in section 3. The corresponding provisions of Art. 16 et seq. DSG apply to processing governed by Swiss law. The current list of the providers used per Offering is available in our consent management platform and in our list of sub-processors.

### 6.9 Retention

Analytical data is retained as follows. Raw event level analytics data is retained for a maximum of 14 months and is then deleted or aggregated. Session recordings and heatmap data are retained for a maximum of 12 months. Company identification and buying intent scores are retained for a maximum of 24 months from the last relevant activity, and are then deleted unless a contract or a pre-contractual relationship has come into existence, in which case the relevant data is retained within the customer or prospect record in accordance with section 16. Consent records are retained for 3 years after the consent ends in order to be able to evidence the lawfulness of the processing.

### 6.10 Your right to object and to withdraw your consent

You have an unconditional right to object, at any time and without giving reasons, to the processing of your personal data for direct marketing purposes, including the profiling described in sections 6.3 and 6.4, pursuant to Art. 21 para. 2 GDPR. If you object, we will cease that processing immediately. You may also object at any time, on grounds relating to your particular situation, to any other processing based on Art. 6 para. 1 lit. f) GDPR pursuant to Art. 21 para. 1 GDPR. Under Swiss law, you may request pursuant to Art. 30 para. 2 lit. b) DSG that we refrain from the processing.

Where the processing is based on your consent, you may withdraw that consent at any time with effect for the future, in our consent management platform, which you can reopen at any time using the icon in the lower left area of our websites. Withdrawal does not affect the lawfulness of the processing carried out up to the point of withdrawal.

To object, please use the consent management platform or send an email to privacy@webpros.com. We also honor recognized opt-out signals transmitted by your browser, including the Global Privacy Control signal, in respect of the sale and sharing of personal information and of targeted advertising, as described in section 18.

Independently of the above, you may prevent or limit the collection of analytical data by deactivating or deleting cookies in your browser, by using the browser setting that requests that no tracking take place, and by using the opt-out mechanisms offered by the individual providers, which are listed in our consent management platform.

## 7. Advertising, Retargeting and Conversion Measurement

We advertise our Offerings on third party platforms and we measure the success of that advertising. Where you have given the corresponding consent for the Marketing cookie category, advertising and measurement technologies are activated on our websites. Depending on the Offering, these include the technologies of Google Ads and the Google advertising network, Meta Platforms, LinkedIn, Microsoft Advertising, Criteo, AdRoll, Reddit, Quora and Capterra. The current list per Offering is available in our consent management platform.

For these purposes the relevant platform receives, in particular, an online identifier, your IP address, the page you visited, and the conversion event that occurred, and it may combine that information with an existing account you hold with that platform and with information it has collected on other websites. This enables interest based advertising and retargeting, meaning that you may be shown advertising for our Offerings on other websites and platforms after visiting our websites, and it enables us to measure how many purchases, trials and inquiries resulted from a given advertisement. We may also transmit audience segment information, and, where you have consented to this, a pseudonymized identifier derived from your email address, in order to build or exclude advertising audiences.

This processing involves profiling for direct marketing purposes and, where the advertising platform acts in its own responsibility, a disclosure of personal data to that platform which under certain United States privacy laws constitutes a sale or a sharing of personal information for cross context behavioral advertising. Section 18 describes the corresponding opt-out rights.

The legal basis for the activation of the advertising technologies and for the transmission of data to the advertising platforms is your consent pursuant to Art. 6 para. 1 lit. a) GDPR in conjunction with Sec. 25 para. 1 TDDDG, Art. 45c FMG, Art. 6 para. 6 DSG and the corresponding national provisions implementing Directive 2002/58/EC. Where an advertising platform acts jointly with us as controller in respect of the measurement, a joint controllership agreement pursuant to Art. 26 GDPR is in place with that platform. Transfers to the United States are safeguarded as described in section 3. You may withdraw your consent at any time in our consent management platform, and you may in addition use the advertising settings and opt-out mechanisms of the relevant platform.

## 8. Use of Cookies and Similar Technologies

### 8.1 Cookies

We use cookies and comparable technologies on our websites. Cookies are small text files that are stored on your device, for example your computer, smartphone or tablet, and which contain certain information. Comparable technologies include local storage, session storage, pixels, tracking pixels, software development kits, device fingerprinting and server side identifiers. Wherever this Privacy Policy refers to cookies, these comparable technologies are covered as well.

You can find out which cookies and comparable technologies we use on the relevant Offering, who provides them, for what purpose, and for how long they are stored, at any time in our consent management platform. You can open the consent banner via the icon in the lower left area of our websites. There you can manage, revoke or adjust your consent in accordance with Sec. 25 para. 1 TDDDG for Germany, Art. 45c FMG and Art. 6 para. 6 DSG for Switzerland, and the corresponding national provisions implementing Directive 2002/58/EC in other jurisdictions. You can also configure your browser to refuse or delete cookies, although this may impair the functionality of our Offerings.

### 8.2 Our cookie consent management platform

To document your selection of cookies and comparable technologies and to comply with our legal obligations, we use a consent management platform. When you visit our website, we ask for your cookie preferences. Your decision is stored in a dedicated cookie. The legal basis for this is Art. 6 para. 1 lit. c)

GDPR and Art. 7 para. 1 DSG for Switzerland, as we are legally required to be able to demonstrate and to manage your consent.

For managing your consents we use the consent management platform Usercentrics, provided by Usercentrics GmbH, Sendlinger Strasse 7, 80331 Munich, Germany. The following data is processed and transmitted to Usercentrics:

- Your consent or rejection, including date, time, language and consent identifier

- Device data, such as browser information and anonymized IP address

The processing of this data is carried out in order to fulfill our legal obligations pursuant to Art. 6 para. 1 lit. c) GDPR and Art. 7 para. 1 DSG for Switzerland. Consent records are retained for 3 years after the consent ends.

Technologies which are not strictly necessary are loaded only after you have given the corresponding consent. This applies in particular to all technologies in the Analytics and Marketing categories, to the interaction analytics described in section 6.5, to the experimentation service described in section 6.6, to the embedded third party content described in section 5.13 and to the advertising technologies described in section 7.

### 8.3 Cookie categories in use by WebPros

We classify cookies and comparable technologies into the following four categories.

| **Cookie types** | **Description** |
|---|---|
| Essential | Essential Cookies help make an Offering usable by enabling basic functions like page navigation and access to secure areas of the Offering. The Offering cannot function properly without these cookies. |
| Functional | Functional Cookies allow the Offering to remember the user's website preferences and choices they make on the Offering including login details, geo-location, language, and enhanced content. This allows the Offering to provide personalized features for users. Functional Cookies are used to enhance the performance of Offerings, as without them, certain functions of the Offerings may not be available. Functional Cookies are helping to provide services that a user requests. |
| Analytics | Analytic Cookies collect information about your use of the Offering and enable us to improve the way it works. These cookies give us aggregated information that we use to monitor site performance, count page visits, spot technical errors, see how users reach the site, and measure the effectiveness of advertising (including emails we send to you). |
| Marketing | Marketing Cookies allow us and other trusted advertisers to select advertisements that are based on your interests, including those expressed or inferred by visits to our Site or apps or across other Offerings, online services, and apps over time. Others help prevent the same advertisement from continuously reappearing for you. These types of cookies also help us provide you with content on the Site that is tailored to your interests and needs. Some Marketing Cookies and other technologies are used in part to also facilitate advertising. Please be aware that Marketing Cookies in some cases have a direct relation to Social Cookies. These Social Cookies are used to enable you to share content, which is a matter of your own interest as well as may participate in the process of authorization via social media services to gain access to 3rd party apps/websites, if you choose to do so. Social cookies may also be used for advertising/analytics purposes. |

Cookies in the Essential category are set on the basis of Art. 6 para. 1 lit. b) and lit. f) GDPR and do not require consent. Cookies in the Functional, Analytics and Marketing categories are set only on the basis of your consent pursuant to Art. 6 para. 1 lit. a) GDPR in conjunction with the applicable national provision implementing Directive 2002/58/EC, and Art. 6 para. 6 DSG for Switzerland. Storage periods range from the duration of the browsing session to a maximum of 24 months and are stated per technology in our consent management platform.

### 8.4 Note on Google Services

We use various services from Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("Google") on our websites, in particular Google Tag Manager, Google Analytics 4, Google Ads and Google reCAPTCHA. This may also involve data transfers to Google LLC, 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA.

For data subjects in the EU, the transfer is based on the EU-U.S. Data Privacy Framework. Google is certified for this and is subject to the adequacy decision of the European Commission for the USA. For Switzerland, the transfer is based on the Swiss-U.S. Data Privacy Framework. Google is also certified for this, so that Switzerland recognizes an adequate level of data protection for transfers to the USA. If, in exceptional cases, there is no certification or adequate protection, we additionally ensure the protection of your data through standard contractual clauses or other suitable measures.

In Google Analytics we have activated IP address truncation, we have deactivated the use of the data for Google's own purposes to the extent that the service permits, and we have concluded the data processing terms offered by Google. Where Google acts as an independent controller in respect of advertising services, section 7 applies.

### 8.5 Offering-specific cookie and technology table

The list of the cookies and comparable technologies used on the specific Offering you are currently visiting, including the provider, the purpose, the category, the storage period and the recipient country for each entry, is as follows:

**[USERCENTRICS]**

## 9. Use of Artificial Intelligence (AI) Features

Some of our websites, products and online services include AI powered features such as chatbots, support assistants, content assistants, AI search and other tools based on large language models ("LLMs") (collectively "AI Features"). This section describes how personal data is processed in connection with these AI Features. AI Features currently in use include the AI support assistant (Zendesk) available in the Plesk, cPanel and WHMCS support portal and the AI content generation features available in SocialBee. The MCP Connector described in section 11.5, through which you may connect an AI assistant of your own choice to your account, is not an AI Feature within the meaning of this section, since the AI assistant is not provided by us. The processing in connection with the MCP Connector is described exclusively in section 11.5.

### 9.1 Data collected and purposes of processing

When you use AI Features, we process the text inputs and prompts you submit, AI generated outputs, and associated usage and technical data such as session identifiers and timestamps. This data is used to provide the requested AI functionality, ensure security, prevent misuse and improve our services. Please do not submit special categories of personal data, for example health, financial or political information, through AI Features.

The legal basis for processing is Art. 6 para. 1 lit. b) GDPR (contract performance) where AI Features form part of a requested service, Art. 6 para. 1 lit. f) GDPR (legitimate interests) for service improvement and

security, and Art. 6 para. 1 lit. a) GDPR (consent) where explicitly required. Under Swiss law, processing is based on Art. 31 para. 1 DSG.

### 9.2 No use of user data for AI model training

We do not use any data submitted through AI Features, including inputs, prompts, conversation content or AI generated outputs, to train, fine tune, retrain or otherwise improve any LLM or AI system, whether operated by us or by any third party provider. We contractually require all AI service providers to uphold this same prohibition.

### 9.3 Third-party AI service providers

AI Features may be powered by third party LLM providers acting as data processors on our behalf. Your input data may be transmitted to such providers solely to deliver the requested service. We require all AI providers to process data only to the extent necessary to provide the service, to implement appropriate technical and organizational security measures, to refrain from using your data to train or improve any AI model, and to comply with applicable data protection law including the GDPR. AI sub-processors and their involvement in certain services are included in the published WebPros list of sub-processors on www.webpros.com. WebPros reserves the right to change or add LLM providers at any time, provided that the safeguards described in this document are fulfilled. International transfers are governed by the mechanisms described in section 3.

### 9.4 AI-assisted outputs and automated processing

AI Features on our websites are informational and assistive in nature. They do not produce legally binding automated decisions within the meaning of Art. 22 GDPR or Art. 21 DSG. Where any AI driven process were to result in decisions with significant legal or similar effect, we would inform you separately and provide the applicable safeguards and rights. Your general rights regarding automated decision making and profiling are set out in section 17.7.

### 9.5 AI chatbot transparency, labeling and access controls

Where AI Features take the form of a chatbot or conversational assistant accessible on our websites or within our products, the following additional measures apply.

(a) Disclosure of AI nature. In accordance with Art. 50 para. 1 of Regulation (EU) 2024/1689 (the "EU AI Act") and applicable national transparency requirements, all chatbot interfaces are clearly and prominently labeled as AI powered prior to or at the commencement of any interaction. Users will not be left under the impression that they are communicating with a human being.

(b) Consent for website-based chatbots. Where a chatbot deployed on our websites processes personal data through technologies that access or store information on the user’s terminal device, for example session cookies, local storage or comparable client side technologies, such processing is subject to prior informed consent in accordance with the applicable national laws implementing Directive 2002/58/EC. Such consent is obtained through our consent management platform before the chatbot widget is activated. Where the chatbot is provided exclusively as part of a logged-in product or support environment and no terminal device storage beyond strictly necessary session management is involved, processing will not require prior consent, provided that no additional tracking technologies are employed.

(c) No automated decisions. Chatbot interactions do not constitute automated decision making within the meaning of Art. 22 GDPR. Chatbot outputs are informational and assistive only. Users are not subject to any decision based solely on automated processing that produces legal or similarly significant effects as a result of their chatbot interaction. Chatbot interaction data is not used for the buying intent scoring described in section 6.4 unless you have given the corresponding consent.

(d) EU AI Act classification. Chatbots of the type deployed by WebPros, meaning general purpose conversational assistants powered by LLMs operating in an informational and support capacity without

producing legal effects, are not classified as high risk AI systems under Annex III of the EU AI Act. They are subject to the transparency obligations set out in Art. 50 EU AI Act. WebPros ensures compliance with these transparency obligations and monitors regulatory developments regarding the classification of LLM based systems under the EU AI Act.

### 9.6 Internal analysis of call transcripts

WebPros uses Gong (Gong.io Inc.) to record and transcribe certain customer facing calls, for example sales and customer success conversations. Recording takes place only where all participants have been informed at the start of the call and have agreed to the recording. For internal quality assurance, coaching and aggregated trend analysis, the textual transcripts generated by Gong are processed by us using the Anthropic Claude large language model. The underlying audio and video recordings are not transmitted to the LLM provider. Anthropic, PBC acts as a contractually bound data processor and is included in our list of sub-processors.

The legal basis for the recording and transcription of the call is your consent pursuant to Art. 6 para. 1 lit. a) GDPR, which is obtained at the start of the call and which you may refuse or withdraw at any time without any disadvantage, in which case the call continues without recording. The legal basis for the subsequent internal analysis of the transcript is Art. 6 para. 1 lit. f) GDPR, based on our legitimate interest in evaluating and improving the quality of customer interactions and our services. For processing governed by Swiss law, Art. 31 para. 1 DSG applies. Where the applicable national law requires the consent of all parties for the recording of a conversation, we record only where that consent has been obtained.

Transcripts are processed only to the extent necessary, are not used to train, fine tune or otherwise improve any Anthropic or third party AI model, and access is restricted to authorized WebPros personnel on a need to know basis. International transfers to Anthropic in the United States are safeguarded by the EU standard contractual clauses pursuant to Art. 46 para. 2 lit. c) GDPR and, where available, an applicable adequacy decision. Recordings and transcripts are retained for a maximum of 24 months. You may object to the analysis at any time pursuant to Art. 21 GDPR.

### 9.7 Data retention and your rights in relation to AI Features

Interaction data from AI Features is retained only as long as necessary to provide the service or as required by law. Session based inputs are generally not retained beyond the active session unless you have an account and session history is an explicit feature. Retention is otherwise governed by section 16. Your rights of access, rectification, erasure, restriction, portability and objection apply equally to data processed through AI Features and are described in section 17. To exercise your rights or raise any AI related privacy concern, please contact privacy@webpros.com.

## 10. Identity Verification and Sanctions Screening

In certain cases we are required to verify the identity of a customer, a partner, a reseller or an authorized representative. This applies in particular where we are subject to know your customer, anti money laundering, sanctions, export control or fraud prevention obligations, where a high value or high risk transaction is concerned, or where a partner or reseller account is onboarded. Separately, and only where we have reasonable doubts as to your identity and no less intrusive means of verification is available to us, we may need to establish your identity before acting on an account recovery request or on a request to exercise your rights as a data subject.

For this purpose we may ask you to provide a copy of an official identity document. The following data may be processed: the image or scan of the document you provide to us, and the name, date of birth, nationality and document number extracted from it. The document is reviewed manually by the WebPros Legal Department in order to compare that data with entries in the applicable sanctions, embargo and denied party lists and, where relevant, in order to confirm your identity. No facial image is recorded, no biometric template is created, and no automated facial comparison, liveness detection or other automated biometric

analysis is carried out. The review and any decision resulting from it are always made by a member of the WebPros Legal Department.

Please redact or mask any information on the document that we have not asked for. Where you provide us with data that is not required for the purposes stated above, we mask it as soon as the review has been completed. Please do not send an identity document by unencrypted email. On request we will make a secure channel available to you for the transmission.

The legal basis is Art. 6 para. 1 lit. c) GDPR in conjunction with the applicable anti money laundering, sanctions and export control provisions, Art. 6 para. 1 lit. b) GDPR where the verification is necessary in order to enter into or to perform the contract, and Art. 6 para. 1 lit. f) GDPR for the prevention of fraud and for the protection of your account and your data where we verify your identity before acting on an account recovery request or on a data subject request. In the latter case Art. 12 para. 6 GDPR applies. Under Swiss law we rely on Art. 31 para. 1 DSG.

Where the applicable anti money laundering or export control law requires us to retain a record of the verification, we retain it for the period prescribed by that law, which is generally 5 to 10 years. In all other cases the copy of the document is deleted as soon as the verification has been completed, and we retain only the fact that a verification took place, its date and its outcome.

If you do not wish to provide an identity document, please contact privacy@webpros.com so that we can agree an alternative form of verification. Where no alternative form of verification is legally sufficient, we may be unable to enter into or to continue the business relationship or, in the case of a data subject request, to act on that request.

## 11. Product Telemetry, License Management, Update Checks and MCP Connector

Our software products communicate with WebPros systems and with the domains listed in section 2 for a number of purposes. This section describes that processing. Where you use our products in the environment of a hosting provider or partner, that partner may additionally act as controller in respect of your use of the product.

### 11.1 License activation, verification and entitlement management

In order to activate a license, to verify entitlement, to prevent license misuse and to determine which updates and extensions you are entitled to, our products transmit license keys, installation identifiers, server IP address and host name, product version and edition, activation status and, where applicable, the identity of the reseller or partner to our license management systems, including manage2.cpanel.net, verify.cpanel.net, the WHMCS license verification endpoint, the Plesk key administrator and partner central systems, and the WebPros account systems. The legal basis is Art. 6 para. 1 lit. b) GDPR for the performance of the license agreement and Art. 6 para. 1 lit. f) GDPR for the prevention of license misuse and piracy. Under Swiss law we rely on Art. 31 para. 1 DSG. License records are retained for the duration of the license and for the statutory retention period thereafter.

### 11.2 Update checks and security notifications

Our products query our update and repository servers in order to determine whether updates, patches and security fixes are available. In doing so, the product version, the operating system, the architecture and the IP address of the requesting server are transmitted and logged. The legal basis is Art. 6 para. 1 lit. b) GDPR and Art. 6 para. 1 lit. f) GDPR, and additionally Art. 6 para. 1 lit. c) GDPR in conjunction with Art. 32 GDPR insofar as the delivery of security updates is a security measure. Under Swiss law we rely on Art. 31 para. 1 DSG.

### 11.3 Product usage telemetry and error reporting

Some of our products collect usage telemetry and error reports in order to understand which functions are used, to detect defects and to prioritize development. In Plesk this is implemented through a user activity tracking function which records the actions carried out in the administration interface together with an installation identifier and a session identifier, stores that data on cloud infrastructure operated by our infrastructure provider, and makes it available for analysis in a product analytics tool. Plesk additionally uses an error and performance monitoring service for the collection of crash and error reports. In WHMCS an analytics function records administration area activity and installation configuration data. Comparable functions may exist in other products and are documented in the respective product documentation.

Where the product documentation designates the telemetry function as optional, it can be deactivated in the product configuration, and in WHMCS it is activated per administrator account. Where telemetry is collected on the basis of our legitimate interest, the legal basis is Art. 6 para. 1 lit. f) GDPR and Art. 31 para. 1 DSG, based on our interest in the quality, security and further development of our products. Where the applicable national law implementing Directive 2002/58/EC requires consent for the storage of an identifier on the terminal device, telemetry is activated only on that basis. Telemetry data is retained for a maximum of 24 months. Error reports are retained for a maximum of 12 months.

Telemetry data collected inside a product installation is not merged with the website analytics described in section 6 for the purpose of the buying intent scoring described in section 6.4 unless the account holder has consented to that use or unless the data has been aggregated so that it no longer relates to an identified or identifiable person.

### 11.4 Data in customer environments

Where personal data of your own customers or end users is contained in a product installation, a control panel, a billing system, a backup set or a support diagnostic file, we process that data solely as a processor on your instructions and on the basis of the applicable data processing agreement. You remain the controller in respect of that data. Where you provide us with a diagnostic file, a database dump or a backup for support purposes, please redact any data that is not required in order to resolve the request.

### 11.5 MCP Connector for AI Assistants

We provide a hosted service based on the Model Context Protocol (the "MCP Connector"), which we operate on our own cloud infrastructure and which is not part of the Plesk or cPanel software installed on your servers. The MCP Connector allows you to connect an AI assistant or another MCP client of your own choice, for example Claude provided by Anthropic, PBC, to your WebPros account or, where you sign in with a cPanel panel token, to your cPanel account. Through the tools offered by the MCP Connector, your AI assistant can read and manage the Plesk and cPanel servers which you have linked to your account, irrespective of where those servers are hosted, and can access information relating to your WebPros account (each such use a "Tool Call"). The connection is established only on your initiative and is authorized through the authentication procedure of the MCP Connector, in the case of the connector listed in the directory of your AI assistant by signing in with your WebPros account. You may end the connection at any time by deleting the API token or MCP key used for the connection in your WebPros dashboard, which takes effect immediately, by changing your password, by disconnecting the relevant server from your WebPros account, or by disconnecting the MCP Connector in your AI assistant. In the latter case the access token is no longer renewed, and access ends no later than 15 minutes after disconnection.

The MCP Connector is operated by WebPros International GmbH, Vordergasse 59, 8200 Schaffhausen, Switzerland, which is the controller for the processing described in this section, without prejudice to paragraph (d) and to the joint processing within the WebPros group described in section 4.

(a) Data processed. For each Tool Call we record the following data in a log:

- The identity of the caller, namely the user identifier, the team identifier and the identifier and name of the API key used or, where you sign in with a cPanel panel token instead of a WebPros account, the account subject identifier of that panel account

- The AI assistant or MCP client software used and the tool called

- The identifier, name and type of the targeted servers

- The input parameters transmitted by your AI assistant to the tool

- The result returned by the tool, which may contain panel data such as domains, mailboxes, user accounts and their settings

- Whether the Tool Call was successful and, where it failed, the error message

- The duration and the timestamps of the Tool Call

Before any data is stored, passwords, tokens, keys, authorization headers, cookies, session identifiers and comparable credentials are masked so that they are not stored in readable form, email addresses are stored only in hashed form, IP addresses are partially masked, error messages are sanitized to remove personal data such as email addresses, and binary content is discarded.

(b) No collection of conversation data. We do not receive, access or store the content of your conversation with your AI assistant, in particular the prompts you enter, your chat history, the memory or conversation summaries of your AI assistant, or files you upload to it. Our tools request only the parameters required for the respective action, for example the target server and the panel function to be executed, and do not request any free text on the context or the reasoning of your conversation. Your AI assistant may nevertheless include information from your conversation in those parameters. Please therefore do not instruct your AI assistant to transmit personal data or confidential information to the MCP Connector which is not required for the requested action.

(c) Purposes and legal bases. We process the data described in paragraph (a) in order to execute the Tool Calls you initiate, to provide the activity log in your dashboard, in which each user sees only the Tool Calls made by that user and their results, to detect, analyze and remedy errors, and to ensure the security of the MCP Connector and of the connected servers, including the investigation of misuse. The legal basis is Art. 6 para. 1 lit. b) GDPR for the provision of the MCP Connector and of the activity log, and Art. 6 para. 1 lit. f) GDPR for troubleshooting, security and abuse prevention, based on our legitimate interest in the reliable and secure operation of the MCP Connector. Under Swiss law we rely on Art. 31 para. 1 DSG. Internal access to the log is restricted to the personnel responsible for the operation and security of the MCP Connector in accordance with section 14.

(d) Data from your server environment and your account. Where the input parameters or results of a Tool Call contain personal data of your own customers, end users or mailbox holders, that data originates from your server environment. We process it in the MCP Connector and in the activity log solely as a processor on your instructions in accordance with section 11.4 and the applicable data processing agreement. Where a hosting provider or other WebPros partner provides your Plesk or cPanel account to you, that partner may additionally act as controller as described in section 2. Information relating to your WebPros account which a Tool Call accesses is processed by us as controller in accordance with section 5.5.

(e) Use of Tool Call data. We use Tool Call data only for the purposes described in paragraph (c). Before we use Tool Call data for any further purpose, we will update this Privacy Policy and, where required by law, obtain your consent.

(f) Provider of your AI assistant. The AI assistant you connect is provided by a third party, for example Anthropic, PBC in the case of Claude. That provider processes your conversation and the data returned by the MCP Connector in its own responsibility, under its own terms and privacy notice, and possibly in the United States or in other third countries. The transmission of data to your AI assistant takes place on your instruction. In this respect the provider of your AI assistant does not act as our processor, section 9.3 does

not apply, and we have no influence on the further processing by that provider. Please consult the privacy notice of the relevant provider for further information.

(g) Retention. The data described in paragraph (a), including the input parameters, the results and the sanitized error messages, is deleted automatically after 30 days by a daily automated deletion run. Deleted records may remain in our database backups for up to a further 35 days until those backups are overwritten in the regular rotation. During that period the backups are not used for any other purpose, and if a backup has to be restored, records whose retention period has expired are deleted again by the next daily deletion run, within 24 hours. A longer retention takes place only where required in an individual case in order to investigate a specific security incident or to establish, exercise or defend legal claims, in which case the relevant records are kept separately with restricted access for as long as necessary for that purpose.

(h) Hosting, recipients and your rights. The MCP Connector and its database, including the backups, are hosted by Amazon Web Services in the European Union (Ireland). For error monitoring we use Sentry, which receives the job identifier and the error description as technical context, without input parameters or results, and removes sensitive data by server-side data scrubbing before storage. Sentry processes this data in the United States. These providers act as our processors and are included in our list of sub-processors. Where a provider processes data outside the EU or the EEA, the transfer is safeguarded as described in section 3. Your rights described in section 17 apply equally to the data processed in connection with the MCP Connector.

## 12. Offering-Specific Provisions

The following provisions apply in addition to the general provisions of this Privacy Policy in respect of the Offering concerned. In the event of a conflict, the Offering specific provision prevails for that Offering.

### 12.1 Plesk

The Plesk websites include a marketing website, a blog, a documentation portal, a Zendesk based support portal with an AI support assistant, a community forum operated on forum software with public member profiles, a training and certification platform with public partner leaderboards, a public feature request board and the Plesk 360 and WebPros Platform 360 account and single sign-on system at platform360.io. Part of the Plesk product range is sold through a reseller of record. Plesk software contains the license management, update check and user activity tracking functions described in section 11. Plesk servers can be connected to an AI assistant through the MCP Connector described in section 11.5. Plesk extensions provided by third parties may set their own cookies inside the product interface, and the relevant extension documentation as well as privacy policy applies to those.

### 12.2 cPanel and WHM

The cPanel websites include a marketing website, a blog, a documentation portal, a Zendesk based support portal including a community area with publicly visible posts, a web shop operated on WHMCS software with its own account and checkout, a training platform, a public feature request board, partner and license management portals, a legacy ticketing system, a first party link redirection service used to measure clicks on links in our communications, and a separate security announcement site. cPanel software contains the license management and update check functions described in section 11. cPanel servers can be connected to an AI assistant through the MCP Connector described in section 11.5.

### 12.3 WHMCS

WHMCS Ltd. is established in the United Kingdom and the UK GDPR applies to its processing in addition to this Privacy Policy. The WHMCS websites include a marketing website, a documentation portal, a developer portal, a client area with checkout and license verification, a marketplace at marketplace.whmcs.com with separate vendor and buyer accounts, an internal wallet and deposit function and the MarketConnect service, a feature request site, a Zendesk based support portal, a download portal,

an accessibility widget, and a community forum operated on separate forum software with its own accounts and publicly visible content. Marketplace vendors are independent third parties and receive the data necessary to fulfill an order for their product. WHMCS software contains the license verification and administration area analytics functions described in section 11. The payment gateways, domain registrars, fraud protection providers and other modules listed on our website are integrations which you as the operator of a WHMCS installation may activate, in which case you determine the resulting processing as controller.

### 12.4 SocialBee

SocialBee LABS SRL is established in Romania. SocialBee is a social media management service. In order to provide the service, SocialBee connects to the application programming interfaces of third party social media and content platforms on your instruction, currently including Facebook, Instagram, Threads, X, LinkedIn, TikTok, YouTube, Pinterest, Bluesky and Google Business Profile, and to content, automation and link management services which you may choose to connect, currently including Canva, Unsplash, GIPHY, Zapier and comparable automation platforms and URL shortening services.

When you connect a social media account, you authorize the connection through the authorization procedure of the relevant platform. SocialBee stores the resulting access and refresh tokens, the account identifier, the profile name and avatar, the permission scopes granted, and the content, scheduling, publication status and performance statistics of the posts you manage through the service. Where a connected platform returns audience or engagement data, that data may include personal data relating to the users who interact with your posts. In respect of that data you act as controller and SocialBee acts as your processor on the basis of the applicable data processing agreement, and you are responsible for having a legal basis for the processing and for informing those users. SocialBee applies the platform terms of the relevant social media platform in addition to this Privacy Policy.

The legal basis for the connection and for the processing of the connected account data is Art. 6 para. 1 lit. b) GDPR for the performance of the contract. You may disconnect a connected account at any time in the application, and you may in addition revoke the authorization in the settings of the relevant platform, in which case the stored tokens are invalidated and deleted. SocialBee provides AI content generation features which are subject to section 9.

SocialBee additionally uses a meeting notetaking service for internal meetings and, on its marketing website, a buyer intent measurement service provided by an independent software review platform, which is subject to section 6.4.

### 12.5 Comet Backup

Comet Licensing Ltd. is established in New Zealand and the New Zealand Privacy Act 2020 applies to its processing in addition to this Privacy Policy. The Comet Backup websites include a marketing website, a documentation portal with a hosted search function, a Zendesk based support portal, a webinar platform, a meeting scheduling service, and an account and single sign-on system at account.cometbackup.com through which trial registration takes place using the WebPros single sign-on.

Comet Backup is backup software. The backup content and the metadata of your backups, including file names, paths and sizes, and the credentials for the storage destination you configure, are processed by you as controller in your own installation. Where you use the storage service offered under the Comet Storage brand, the underlying object storage is provided by a third party storage provider acting as our sub-processor, and we act as your processor in respect of the stored content on the basis of the applicable data processing agreement. Where you configure a third party storage destination such as an object storage service of another provider, that provider acts on your instruction and its own terms apply. Backup content is encrypted, and where you manage the encryption keys yourself we have no ability to access the content. Comet Backup software contains the license management and update check functions described in section 11, and it can be integrated with third party billing, monitoring and remote management systems which you may choose to activate, in which case you determine the resulting processing as controller.

### 12.6 XOVI

XOVI is a search engine and LLM search optimization and online marketing product. It is operated and sold by WebPros Germany GmbH, which is the controller for that Offering. The XOVI websites include a marketing website, a documentation and help portal, a customer account with subscription and billing functions, and the XOVI application. Where the XOVI Offering uses a consent management platform, an analytics provider, an advertising technology or a support platform other than those named in this Privacy Policy, the provider concerned is identified in the consent management platform on that website and in our list of sub-processors, and the general provisions of sections 5 to 8 of this Privacy Policy apply accordingly.

## 13. Recipients of personal data

We disclose personal data only to the extent necessary and only to recipients, who have a need to know of the information in order to allow us to provide the services or for other legally permitted purposes under applicable privacy laws.

The categories of recipients may be the following (full list - not all apply in each specific case).

- Companies within the WebPros group, as described in section 4

- Cloud infrastructure, hosting, content delivery and security providers

- Customer relationship management, marketing automation and email delivery providers

- Analytics, tag management, interaction analytics and experimentation providers, and company identification and business intent data providers

- Advertising, retargeting and conversion measurement platforms, as described in section 7

- Consent management platform providers

- Support desk, knowledge base, community platform, learning management, webinar and event providers

- Resellers of record, payment service providers, subscription billing providers and collection agencies

- Affiliate and partner program platform providers

- Sanctions, export control and fraud screening providers

- Large language model and AI service providers, as described in section 9

- Providers of AI assistants and other MCP clients which you choose to connect to the MCP Connector, which receive data on your instruction and in their own responsibility, as described in section 11.5

- Human resources, applicant tracking and payroll providers, in respect of applicant and employee data

- Auditors, tax advisers, attorneys, insurers and other professional advisers bound by professional secrecy

- Public authorities, courts and law enforcement bodies, where we are legally obliged to disclose or where disclosure is necessary in order to establish, exercise or defend legal claims

- Acquirers or prospective acquirers and their advisers, in the context of a merger, acquisition, reorganization or sale of assets, subject to appropriate confidentiality safeguards

- Hosting providers, resellers, managed service providers and other WebPros partners, in respect of the customer relationship they maintain with you

Every recipient acting on our behalf is bound by a data processing agreement in accordance with Art. 28 GDPR and Art. 9 DSG. The current list of our sub-processors, including the WebPros brands to which each sub-processor is allocated and the country in which it processes data, is published in the legal section of www.webpros.com. We do not sell personal data. Section 18 describes the treatment of disclosures which constitute a sale or a sharing of personal information under United States privacy laws.

## 14. Data Security and Notification of Data Breaches

We implement appropriate technical and organizational measures pursuant to Art. 32 GDPR and Art. 8 DSG in order to protect your personal data against unauthorized or unlawful processing and against accidental loss, destruction or damage. These measures include transport encryption of our websites and services, encryption of data at rest, role based access control and the least privilege principle, multi factor authentication for administrative access, network segmentation, logging and monitoring, vulnerability management and patching, secure software development practices, regular penetration testing, background screening of personnel where lawful, confidentiality undertakings, security awareness training, supplier security assessment and a documented incident response process. Our security posture is subject to periodic re-assessment.

Notwithstanding these measures, the transmission of information over the internet cannot be guaranteed to be completely secure. Please use a strong and unique password for your account, enable multi factor authentication where offered, and inform us without delay at security@webpros.com if you become aware of a suspected security incident or vulnerability affecting our Offerings.

In the event of a personal data breach we will notify the competent supervisory authority without undue delay and, where feasible, within 72 hours of becoming aware of it, in accordance with Art. 33 GDPR, and we will notify affected data subjects in accordance with Art. 34 GDPR where the breach is likely to result in a high risk to their rights and freedoms. Corresponding notifications are made to the Federal Data Protection and Information Commissioner in accordance with Art. 24 DSG, to the Information Commissioner's Office in accordance with the UK GDPR, and to the Office of the Privacy Commissioner in accordance with the notifiable privacy breach provisions of the New Zealand Privacy Act 2020, and under the other applicable regimes referred to in section 18. Where we act as a processor, we will notify the relevant controller without undue delay in accordance with Art. 33 para. 2 GDPR and the applicable data processing agreement.

## 15. Children's Data

Our Offerings are directed at businesses and at professional users and are not directed at children. We do not knowingly collect personal data from children under the age of 16, or under the higher age of consent applicable in the relevant jurisdiction. If you believe that a child has provided personal data to us, please contact privacy@webpros.com and we will delete that data without undue delay. We do not knowingly sell or share the personal information of any consumer under 16 years of age within the meaning of the applicable United States privacy laws.

## 16. Duration of Data Processing

We store personal data only as long as it is necessary to achieve the respective purpose or until you withdraw your consent. The specific retention periods for the individual processing activities are stated in the relevant sections of this Privacy Policy. Where no period is stated, we retain the data for as long as is necessary for the purpose described, and the criteria we apply are the continued existence of the contractual or pre-contractual relationship, the applicable statutory retention obligations and the applicable limitation periods.

If there are legal retention obligations, for example under commercial, tax or social security law in Switzerland, the EU, the United Kingdom, the United States or New Zealand, the retention of certain data may be required for up to 10 years or longer, regardless of the processing purpose. Data which is required in order to establish, exercise or defend legal claims is retained until the expiry of the applicable limitation period.

To ensure that no data is stored longer than necessary, we operate a deletion concept, we conduct regular reviews and we delete or anonymize personal data as soon as the purpose of storage ceases to exist and there are no legal obligations or overriding legitimate interests remaining.

# 17. Your Rights as a Data Subject

### 17.1 Request for information and access

Upon request, you can receive information about the personal data we have stored about you, the purposes of the processing, the categories of data concerned, the recipients or categories of recipients, the envisaged retention period, the origin of the data where it was not collected from you, and the safeguards applied to any third country transfer. The first copy is provided free of charge. For further copies we may charge a reasonable fee covering our administrative costs, and we may refuse or charge for manifestly unfounded or excessive requests, in accordance with Art. 12 para. 5 GDPR and Art. 19 of the Swiss Data Protection Ordinance.

### 17.2 Rectification, erasure and restriction of processing

If you no longer agree with the storage of your personal data, or if the data has become incorrect, we will delete or restrict your data upon your instruction or make the necessary corrections, as far as this is possible under applicable law. The same applies if we should only process data in a restricted manner in the future.

### 17.3 Right to object

You have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data which is based on Art. 6 para. 1 lit. e) or lit. f) GDPR, including profiling based on those provisions, pursuant to Art. 21 para. 1 GDPR. Where your personal data is processed for direct marketing purposes, you have an unconditional right to object at any time and without giving reasons, including in respect of the profiling described in section 6, pursuant to Art. 21 para. 2 GDPR. Following such an objection your personal data will no longer be processed for those purposes. Under Swiss law, you may request pursuant to Art. 30 para. 2 lit. b) DSG that we refrain from a particular processing.

### 17.4 Right to withdraw consent with effect for the future

You can withdraw your consent at any time with effect for the future, without giving reasons and without any disadvantage. Withdrawal is as easy as giving consent, and for consent relating to cookies and comparable technologies you may withdraw it in our consent management platform, which you can reopen at any time using the icon in the lower left area of our websites. Your withdrawal will not affect the lawfulness of the processing carried out up to the time of withdrawal.

### 17.5 Data portability

If data processing is based on a contract or on your consent and is carried out by automated means, you have the right to data portability. Upon request we will provide the data you provided to us in a common, structured, commonly used and machine readable format, so that you can transfer the data to another controller if desired.

### 17.6 Data which cannot be attributed to you

Data for which we are unable to identify the data subject, for example because it has been anonymized or aggregated for analysis purposes, is not covered by the aforementioned rights. If you provide us with additional information that allows us to identify you, we will give effect to your rights in respect of that data. Where we are unable to identify you from the information available to us, we will inform you accordingly in accordance with Art. 11 para. 2 GDPR.

### 17.7 Profiling, automated decision-making and scoring

Some of our offerings carry out profiling within the meaning of Art. 4 no. 4 GDPR in the cases described in section 6 and section 7 of this Privacy Policy, namely the analysis of your website activity, the identification of the company on whose behalf you act, the determination of buying intent signals and lead prioritization,

the interaction analytics described in section 6.5, and the interest based advertising described in section 7. That profiling is carried out on the basis of your consent, or on the basis of our legitimate interest as set out in section 6.7, and you have an unconditional right to object to it insofar as it serves direct marketing purposes.

Your data is not used by us for automated decisions which have legal consequences for you or which significantly affect you in a similar way, as described in Art. 22 GDPR and Art. 21 DSG. In particular, no price, no product availability, no contractual term, no credit decision and no eligibility decision is determined solely by automated means. Where we exceptionally introduce automated decisions of that kind, we will inform you transparently in advance, we will obtain your explicit consent where required, and we will provide you with the right to obtain human intervention, to express your point of view, to receive an explanation and to contest the decision.

### 17.8 Exercising your rights and right to lodge a complaint

If you have any questions regarding the processing of your personal data, or if you wish to exercise a right of access, rectification, erasure, restriction, objection, withdrawal of consent or portability, please contact privacy@webpros.com. We will respond without undue delay and in any event within one month of receipt of the request, and we may extend that period by a further two months where the request is complex, in which case we will inform you of the extension and the reasons for it. In order to protect your data we may need to verify your identity before acting on a request, and we will request only the information necessary for that purpose. You may act through an authorized agent, in which case we will require evidence of the authorization.

You also have the right to lodge a complaint with a supervisory authority. In the case of a WebPros company based in Switzerland you may complain to the Federal Data Protection and Information Commissioner (FDPIC), Feldeggweg 1, 3003 Bern, Switzerland. If you are located in the EU or the EEA you may complain to the supervisory authority of your habitual residence, your place of work or the place of the alleged infringement. Further authorities are named in section 18. Lodging a complaint does not affect any other administrative or judicial remedy.

## 18. Supplementary Country and Regional Provisions

The following provisions apply in addition where the law of the relevant jurisdiction applies to the processing of your personal data.

### 18.1 European Union and European Economic Area

Where a WebPros entity established outside the EU and the EEA offers goods or services to, or monitors the behavior of, data subjects in the EU or the EEA within the meaning of Art. 3 para. 2 GDPR, that entity has designated WebPros Germany GmbH, Hohenzollernring 72, 50672 Cologne, Germany, as its representative in the Union pursuant to Art. 27 GDPR. You may contact the representative at privacy@webpros.com in respect of all issues related to the processing of your personal data. The competent supervisory authorities of the WebPros entities established in the EU include the data protection authority of North Rhine-Westphalia for Germany, the Agencia Española de Protección de Datos for Spain, the Commission for Personal Data Protection for Bulgaria, the Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal for Romania. You may lodge a complaint with the authority of your habitual residence or place of work irrespective of which entity carried out the processing.

### 18.2 United Kingdom

The UK General Data Protection Regulation and the Data Protection Act 2018 apply to the processing carried out by WHMCS Ltd. and to processing relating to data subjects in the United Kingdom. References in this Privacy Policy to provisions of the GDPR are to be read as references to the corresponding provisions of the UK GDPR. Transfers of personal data out of the United Kingdom are safeguarded by the UK Extension

to the EU-U.S. Data Privacy Framework where the recipient is certified, by the International Data Transfer Agreement or by the International Data Transfer Addendum to the EU standard contractual clauses, or by an applicable adequacy regulation. Where a WebPros entity established outside the United Kingdom is subject to the UK GDPR, WHMCS Ltd. acts as its representative in the United Kingdom pursuant to Art. 27 UK GDPR. You have the right to lodge a complaint with the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, United Kingdom.

### 18.3 Switzerland

The Swiss Federal Act on Data Protection applies to processing carried out by WebPros International GmbH and to processing relating to data subjects in Switzerland. The competent authority is the Federal Data Protection and Information Commissioner, Feldeggweg 1, 3003 Bern, Switzerland.

### 18.4 United States: Data Privacy Framework

The provisions applicable to the Data Privacy Framework are set out in section 3.2.

### 18.5 California

If you are a California resident, the California Consumer Privacy Act as amended by the California Privacy Rights Act ("CCPA") may provide you with additional rights regarding our use of your personal information.

Categories of personal information collected. In the preceding 12 months we have collected the following categories of personal information as enumerated in the CCPA: identifiers, including name, postal address, email address, telephone number, account name, internet protocol address and unique online and device identifiers. Personal information categories listed in the California Customer Records statute, including name, address, telephone number and payment information. Commercial information, including records of products or services purchased, licenses held, subscription status and purchasing or consuming histories or tendencies. Internet or other electronic network activity information, including browsing history, search history and information regarding your interaction with our websites, applications and advertisements. Geolocation data, in the form of approximate location derived from your IP address. Professional or employment related information, including your employer, your job title and your business function. Audio and visual information, in the form of call recordings where you have agreed to the recording and, in the identity verification process described in section 10, the image or scan of an identity document. Inferences drawn from the above in order to create a profile reflecting preferences, characteristics, predispositions, behavior and aptitudes, in particular the company assessment and the buying intent score described in sections 6.3 and 6.4. Sensitive personal information, limited to account log-in credentials in combination with the credential required to access the account, government identifiers processed for identity verification purposes as described in section 10, and any information revealing a disability which you voluntarily provide by activating an accessibility profile as described in section 5.11.

Sources, purposes and disclosures. We collect this information directly from you, automatically from your device and your interaction with our Offerings, from our group companies, from our partners and resellers, and from publicly available and commercially available business data sources. We use it for the business and commercial purposes described in this Privacy Policy, in particular in sections 5, 6, 7, 9, 10 and 11. We disclose it for business purposes to the categories of recipients listed in section 13.

Sale and sharing. We do not sell personal information for monetary consideration. However, the use of the advertising and analytics technologies described in sections 6 and 7 may constitute a sale or a sharing of personal information for cross context behavioral advertising under the CCPA, in respect of the categories identifiers, internet or other electronic network activity information, commercial information, geolocation data, professional information and inferences. We do not sell or share sensitive personal information, and we do not use or disclose sensitive personal information for purposes other than those permitted by the CCPA without a right to limit. We do not sell or share the personal information of consumers we know to be under 16 years of age.

Your California rights. You have the right to know and to access the specific pieces and categories of personal information we have collected about you, the right to request deletion, the right to request correction of inaccurate personal information, the right to opt out of the sale and sharing of your personal information, the right to limit the use and disclosure of sensitive personal information, the right to opt out of automated decision making technology to the extent provided by the applicable regulations, and the right not to receive discriminatory treatment for exercising any of these rights. We do not offer financial incentives for the retention or sale of personal information.

How to exercise your rights. You may exercise these rights by contacting privacy@webpros.com or by writing to the address stated below. You may opt out of the sale and sharing of your personal information by adjusting your preferences in our consent management platform, which you can reopen at any time using the icon in the lower left area of our websites, and by disabling the Marketing and Analytics categories. We also recognize and honor the Global Privacy Control opt-out preference signal transmitted by your browser or extension. You may use an authorized agent to submit a request, in which case we will require written authorization and may require you to verify your identity directly. We will respond within the periods prescribed by the CCPA, and you may appeal a decision by contacting privacy@webpros.com with the subject line "Privacy Appeal".

Shine the Light. Pursuant to California Civil Code Section 1798.83, residents of the State of California have the right to request from companies conducting business in California certain information relating to third parties to which the company has disclosed certain categories of personal information during the preceding year for the third parties' direct marketing purposes. Alternatively, the law provides that a company may comply, as WebPros does, by disclosing in its privacy policy that it provides consumers with a choice regarding the sharing of personal information with third parties for those third parties' direct marketing purposes, and information on how to exercise that choice. As stated in this Privacy Policy, WebPros provides you with that choice before sharing your personal information with third parties for their direct marketing purposes. If you do not opt in, or if you choose to opt out at the time WebPros offers that choice, WebPros does not share your information with the identified third party for its direct marketing purposes.

If you are a California resident and you have questions about our practices with respect to sharing information with third parties for their direct marketing purposes and your ability to exercise choice, please send your request to privacy@webpros.com or write to us at the following mailing address:

WebPros International, LLC

Attention: Privacy
1100 W 23rd St
Suite 153
Houston TX, 77008
legal@webpros.com

Please put the statement "Your California Privacy Rights" in the subject field of your email, or include it in your letter if you choose to write to us at the designated mailing address. You must also include your name, street address, city, state and ZIP code. We are not responsible for notices that are not labeled or sent properly, or that do not contain complete information.

**18.6 Other United States states**

Comprehensive state privacy laws also apply in a number of other states, including Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, Florida, Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, Maryland, Indiana, Kentucky and Rhode Island, and further states as their laws come into effect. If you are a resident of one of those states, you have, subject to the specific provisions and exemptions of your state law, the right to confirm whether we process your personal data and to access that data, the right to correct inaccuracies, the right to request deletion, the right to obtain a portable copy, the right to opt out of targeted advertising, of the sale of personal data and of profiling in furtherance of decisions that produce legal or similarly significant effects, and the right not to be discriminated against for

exercising those rights. We obtain your consent before processing sensitive data where your state law requires it.

As described in sections 6 and 7, we process personal data for targeted advertising and we engage in disclosures that may constitute a sale of personal data under these laws. We do not use profiling in furtherance of decisions that produce legal or similarly significant effects. You may exercise your opt-out rights through our consent management platform, through the Global Privacy Control signal, or by contacting privacy@webpros.com. Where your state law provides a right of appeal against our decision on a request, you may appeal by contacting privacy@webpros.com with the subject line "Privacy Appeal", and if the appeal is denied you may contact your state attorney general.

### 18.7 Romania

SocialBee LABS SRL is established in Romania. The competent supervisory authority is the Autoritatea Naţională de Supraveghere a Prelucrării Datelor cu Caracter Personal, B-dul G-ral. Gheorghe Magheru 28-30, Sector 1, 010336 Bucharest, Romania.

### 18.8 New Zealand

Comet Licensing Ltd. is established in New Zealand and the Privacy Act 2020 and the information privacy principles set out in it apply to its processing. You have the right to request access to and correction of your personal information under information privacy principles 6 and 7. Personal information is disclosed outside New Zealand only where the recipient is subject to comparable safeguards in accordance with information privacy principle 12. You may complain to the Office of the Privacy Commissioner, PO Box 10094, The Terrace, Wellington 6143, New Zealand.

### 18.9 Japan

WebPros Japan K.K. is established in Japan and the Act on the Protection of Personal Information applies to its processing. You may request disclosure, correction, suspension of use or deletion of your retained personal data by contacting privacy@webpros.com. The competent authority is the Personal Information Protection Commission.

### 18.10 Canada

Canada WebPros International, Ltd. is established in Canada and the Personal Information Protection and Electronic Documents Act, together with any applicable provincial privacy legislation, applies to its processing. You may complain to the Office of the Privacy Commissioner of Canada or to the competent provincial authority.

### 18.11 India

WebPros (India) Pvt. Ltd. is established in India and the Digital Personal Data Protection Act, 2023 applies to its processing as and when the relevant provisions are brought into force. You may contact privacy@webpros.com in order to exercise your rights to access, correction, completion, updating, erasure and grievance redressal, and to nominate another individual to exercise your rights.

## 19. Changes to this Privacy Policy

This Privacy Policy is subject to periodic revision and may be amended by WebPros from time to time if necessary, in particular where our Offerings, the technologies we use or the applicable law change. The version number and the date of the last update are stated at the beginning of this document. Where an amendment is material and affects the processing of your personal data, we will inform you by an appropriate means before the amendment takes effect, for example by a notice on our websites, by email or in your account, and we will obtain your consent again where the amendment requires it. Please review

this Privacy Policy periodically for updates. Previous versions are available on request from privacy@webpros.com.