

WebPros Privacy Policy

v.15 - Updated May 28th, 2026

A. 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. E.g. for Europe, both, the provisions of the GDPR and the provisions of the Swiss Data Protection Act (DSG) and the UK General Data Protection Regulation (for WHMCS) apply, whereas 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 (e.g. "processing" or "personal data"), these are to be understood as having the same meaning in the sense of the Swiss DSG and/or 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.

B. 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 labelled 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 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.

Supplementary in accordance with Swiss data protection law:

Subjects resident in Switzerland or as far 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 (e.g. the EU Member States, Japan, Canada 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 fulfil a contract or if you have given your express consent.

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 and/or the Swiss-U.S. DPF Principles, these DPF Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, please visit <https://www.dataprivacyframework.gov/> and to view our certification.

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

Pursuant to the Data Privacy Framework (DPF) program, EU, UK, and Swiss you have the right to obtain our confirmation of whether we maintain personal information relating to you 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 Data Privacy Framework (DPF) program, should direct their query to privacy@webpros.com. If requested to remove data, we will respond within a reasonable timeframe, respecting the given legal boundaries.

Before sharing your data with third parties other than our agents, or before using it for a purpose other than the one which it was originally collected for 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.

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 Data Privacy Framework (DPF) program and subsequently transfer to a third party is described in the Data Privacy Framework (DPF) program principles. Categories of third parties that could be involved in the transfer or processing of your data can be viewed in section 6 of this Privacy Policy. These might include online advertisers of our company and product services, website visitor analytics provider or sales target intelligence providers. Each third party which is entrusted with personal data is bound by a Data Processing Agreement in accordance with data protection laws in effect. In particular, we remain responsible and liable under the Data Privacy Framework (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 Data Privacy Framework (DPF) program. European Union, United Kingdom, and Swiss individuals with Data Privacy Framework (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 have further committed to refer unresolved privacy complaints under the Data Privacy Framework (DPF) program Principles to an independent dispute resolution mechanism, Better Business Bureau (“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.

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>

Supplementary in accordance with data protection laws in California / USA:

If you are a California resident, California law may provide you with additional rights regarding our use of your personal information. 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 (opt-out or opt-in) regarding sharing Personal Information with third parties for those third parties’ direct marketing purposes, and information on how to exercise that choice. As stated above in this Privacy Policy, Webpros provides you choice prior to 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 cPanel offers that choice, cPanel does not share your information with that 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 the following email address: [privacy \[at\] cpanel.net](mailto:privacy[at]cpanel.net) 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 e-mail 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 labelled or sent properly, and do not have complete information.

C. Joint Data Processing within the WebPros group

1. Joint Data Processing

As part of our business operations and the use of our website, 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.

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 Netherlands B.V (i.L.), Schiphol Boulevard 369, Tower F, 7th floor, 1118BJ Schiphol / NL
WebPros (India) Pvt. Ltd., B 205, Bldg-42, B-Wing, Azad Nagar Sangam CHS, Andheri, Mumbai, Mumbai- 400053, Maharashtra / India
Canada WebPros International, Ltd., 1055 Dunsmuir Street, Suite 3000, Vancouver, BC V7X 1K8 / Canada
XOVI GmbH, Hohenzollernring 72, 50672 Cologne / Germany
SocialBee Labs Srl., Poet Grigore Alexandrescu Str, No 51, 400560, Cluj-Napoca / Romania
Comet Licensing Ltd., 1/52 Acheron Drive, Upper Riccarton, Christchurch, 8041 / 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. If you have any questions or wish to exercise your rights, the WebPros company you first contacted is usually your point of contact.

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.

3. Contact details of the data protection officer of WebPros International GmbH

Email: privacy@WebPros.com

D. Data Processing

The individual data affected by joint data processing, processing purposes, legal bases, recipients and, if applicable, transfers to third countries are listed below:

1. Contacting WebPros

When you contact us, we process the data you provide to us - for example, your name, your contact details (if provided), and your message - to handle your request. The processing is based on our contractual or pre-contractual obligations (Art. 6 para. 1 b) GDPR) or because we have a legitimate interest in responding

to your inquiry (Art. 6 para. 1 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).

2. Contact in case of Job Applications

If you send us your application, for example, by email or via a contact form, 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.

For companies based in the EU, data processing is carried out on the basis of Art. 6 para. 1 b) GDPR, with § 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 f) GDPR (legitimate interests).

For applications in Switzerland, Art. 328b OR applies. According to this, 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 (e.g., for an applicant pool), or further retention is required to protect legitimate interests (e.g., to defend against claims).

3. Contract fulfilment and data management in the context of service provision

For the establishment, execution, and processing of contracts, we process the necessary data (e.g., name, contact details, address, email address, phone number, access 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 b) and c) GDPR and the corresponding provisions of the Swiss Data Protection Act (DSG) for contract fulfillment and compliance with legal obligations.

If necessary for contract processing, we transmit data to third parties, e.g., 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.

4. Log files of Website Visits

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

- The name(s) of our accessed website(s)
- The date and time of access
- The amount of data transferred
- The browser type and version
- The operating system you use
- The referrer URL (the previously visited website)
- Your IP address
- The requesting provider.

The legal basis for data processing is our overriding legitimate interest in the continuous provision and security of our website in accordance with Art. 6 para. 1 f) GDPR. The log file is deleted after seven days unless it is needed to prove or clarify specific legal violations that have become known within the retention period.

5. Newsletter and Customer Information

To keep you regularly informed about our company and our offers, we offer several email newsletters. For this purpose, we process the data you provide during registration (email address and any voluntary information).

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

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, an EU standard contractual clause exists. European branch: HubSpot Ireland Ltd., 30 North Wall Quay, Dublin 1, Ireland.

Based on WebPros' legitimate interest in accordance with Art.6 para. 1 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. 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.

6. Use of Cookies

We use cookies on our website. These are small text files that are stored on your device (e.g., PC, smartphone, or tablet) and contain certain information. You can find out which cookies we use, who provides them, and for what purpose at any time in our consent management platform. You can open this banner via the icon at the bottom left of our websites. There, you can manage, revoke, or adjust your consent in accordance with § 25 para. 1 TDDDG (Germany) and Art. 6 para. 6 DSG (Switzerland).

6.1. Our Cookie Consent Management Platform

To document your selection of cookies and similar technologies and to comply with our legal obligations, we use a consent management platform (Usercentrics). When you visit our website, we ask for your cookie preferences. Your decision is stored in a special cookie. The legal basis for this is Art. 6 para. 1 lit. c GDPR and Art. 7 para. 1 DSG (Switzerland), as we are legally required to prove and 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, consent ID)
- Device data (such as browser information and anonymized IP address)

The processing of this data is also carried out to fulfill our legal obligations according to Art. 6 para. 1 lit. c GDPR and Art. 7 para. 1 DSG (Switzerland).

6.2. Cookie categories in use by WebPros (Essential, Functional, Analytics, Marketing)

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 3 rd party apps/websites, if you choose to do so. Social cookies may also be used for advertising/analytics purposes.

6.3. Note on Google Services

We use various services from Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("Google") on our website. 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 EU Commission's adequacy decision for the USA.

For Switzerland, the transfer is based on the Swiss-U.S. Data Privacy Framework (Swiss DPF). Google is also certified for this, so 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 (SCC) or other suitable measures.

Search Function and Google Analytics

When you use the search function on our websites, the terms you enter may be shared with Google Analytics, irrespective from any consent given within our cookie banner. This helps us understand how visitors interact with our site and improve its functionality and content. The data shared is used solely for analytical purposes and can not include personally identifiable information. By using the search feature, you consent to this processing and sharing of data with Google Analytics. This practice is consistent with applicable privacy laws and does not constitute a violation of the California Invasion of Privacy Act (CIPA) or other legal frameworks, as it is limited to operational analytics and does not involve unlawful interception of communications. Furthermore, you agree that the information you enter is not a "private communication" under CIPA. For more details on how Google processes data, please review Google's Privacy Policy.

6.4 This specific Offering uses the following cookies and other technologies

<https://cometbackup.com/privacy-policy/#usercentrics>

E. Use of Artificial Intelligence (AI) Features

Some of our websites, products and online services include AI-powered features such as chatbots, content assistants, 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.

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 (e.g. session identifiers, 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 (e.g. 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.

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 large language model 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.

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: (i) process data only to the extent necessary to provide the service; (ii) implement appropriate technical and organizational security measures; (iii) refrain from using your data to train or improve any AI model; and (iv) comply with applicable data protection law, including the GDPR. AI sub-processors are included in the WebPros list of sub-processors, available [here](#). Currently, AI Features are powered by OpenAI. WebPros reserves the right to change or add LLM providers at any time, provided the required safeguards, described in this documents are fulfilled. International transfers are governed by the mechanisms described in the “Third Country Transfer” section of this Policy.

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 the “No Automated Decision-making or Profiling” section of this Policy.

5. AI Chatbot Transparency, Labelling, 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 (“EU AI Act”) and applicable national transparency requirements, all chatbot interfaces are clearly and prominently labelled 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 (e.g. session cookies, local storage, or similar client-side technologies), such processing is subject to prior informed consent in accordance with the provisions of applicable national laws implementing Directive 2002/58/EC (ePrivacy Directive). Such consent is obtained through our consent management platform (Usercentrics) before the chatbot widget is activated. Where the chatbot is provided exclusively as part of a logged-in product environment and no terminal device storage beyond strictly necessary session management is

involved, processing will not require prior consent, provided no additional tracking technologies are employed.

(c) No automated decisions or profiling: Chatbot interactions do not constitute automated decision-making within the meaning of Art. 22 GDPR and do not involve profiling. 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.

(d) EU AI Act classification: Chatbots of the type deployed by WebPros — i.e. 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 may, however, qualify as general-purpose AI systems 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.

6. Internal Analysis of Gong Call Transcripts

If specifically approved in advance by all participants, WebPros uses Gong (Gong.io Inc.) to record and transcribe certain customer-facing calls (e.g., sales and customer success conversations). For internal quality assurance, coaching, and aggregated trend analysis, the textual transcripts generated by Gong (the underlying audio and video recordings are not transmitted) are processed by us using the Anthropic Claude large language model. Anthropic, PBC acts as a contractually bound data processor and is included in our list of sub-processors. The legal basis is Art. 6 para. 1 lit. f) GDPR (legitimate interest in evaluating and improving the quality of customer interactions and our services); for Swiss-law-governed processing, Art. 31 para. 1 DSG. 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. The recording and transcription of calls is separately disclosed at the start of each call; you may object to this processing at any time pursuant to Art. 21 GDPR.

7. AI-Based Identity Verification

Overview and Scope

In certain contexts — such as account registration, onboarding, or compliance with regulatory Know Your Customer (KYC) / Anti-Money Laundering (AML) or export sanctions requirements — WebPros may offer the option of identity verification using AI-based identity verification solutions (“Identity Verification Solutions”), such as iDenfy or comparable services. This section applies exclusively to those situations in which an Identity Verification Solution is actually used, and only where you have given explicit prior consent as described below. Where no such consent is given, Identity Verification Solutions will not be deployed.

Explicit Consent as Prerequisite

The use of any Identity Verification Solution is strictly conditional on your freely given, specific, informed, and unambiguous prior consent in accordance with Art. 6 para. 1 lit. a) and Art. 9 para. 2 lit. a) GDPR. Before commencing any verification process, you will be clearly informed of: (i) the identity of the Identity Verification Solution provider acting as a data processor; (ii) the categories of personal data to be collected and processed, including biometric data; (iii) the automated nature of the verification process and the possible legal or similarly significant effects of the result; (iv) the right to refuse consent without suffering any disadvantage from doing so, including the availability of alternative verification methods where technically and legally feasible; and (v) the right to withdraw consent at any time prior to completion of the verification process, with no prejudice to the lawfulness of processing already carried out. Consent is obtained through a dedicated, separate opt-in step and is documented in our consent management system. No pre-ticked boxes or bundled consent will be used.

Categories of Personal Data Processed

Depending on the verification method chosen and the regulatory requirements applicable to the specific use case, Identity Verification Solutions may process the following categories of personal data: (a) government-issued identity document data (e.g. name, date of birth, document number, nationality, expiry date); (b) facial biometric data, including a real-time or uploaded photograph or video and a derived biometric template used solely to compare the live image with the identity document (“liveness check”); (c) metadata associated with the submission (e.g. device type, IP address, timestamp, session identifier); and (d) the verification result (e.g. verified, rejected, or flagged for manual review). Biometric data constitutes a special category of personal data within the meaning of Art. 9 GDPR and is processed exclusively on the basis of explicit consent as described above. Facial biometric templates are not retained after the verification process is completed beyond the minimum period technically necessary to deliver the result, unless separate explicit consent for retention has been obtained or retention is required by applicable law.

Automated Decision-Making in the Context of Identity Verification

By way of exception to the general statement in the “No Automated Decision-making or Profiling” section of this Policy, and exclusively where you have given explicit prior consent as described above, Identity Verification Solutions involve automated processing that may produce a result — such as identity confirmed, identity not confirmed, or flagged for further review — which may have a legal or similarly significant effect on your access to the requested service. Such processing constitutes automated decision-making within the meaning of Art. 22 GDPR (EU) and Art. 21 DSG (Switzerland). You are entitled to the following safeguards: (i) the right to obtain human review of the automated result by a qualified WebPros employee, upon request made to privacy@webpros.com; (ii) the right to express your point of view and to contest the result; and (iii) the right not to be subject to a decision based solely on automated processing if explicit consent is withdrawn before a final result is communicated. WebPros will not use Identity Verification Solution outputs as the sole basis for a decision that produces significant legal effects without the option of human review unless you explicitly waive this right after being fully informed.

AI Act Compliance — Classification and Obligations

AI-based identity verification systems that perform biometric identification or verification of natural persons are classified as high-risk AI systems under Annex III of Regulation (EU) 2024/1689 (“EU AI Act”). Where WebPros deploys or uses an Identity Verification Solution that falls within this classification, WebPros, in its capacity as deployer within the meaning of Art. 3 no. 4 EU AI Act, ensures compliance with the following obligations applicable to deployers of high-risk AI systems: (a) Use in accordance with the provider’s instructions for use (Art. 26 para. 1 EU AI Act); (b) Assignment of appropriate human oversight to qualified personnel prior to putting the system into use (Art. 26 para. 2 EU AI Act); (c) Monitoring the operation of the system on the basis of the instructions for use (Art. 26 para. 5 EU AI Act); (d) Implementation of a fundamental rights impact assessment prior to deployment, where required under Art. 27 EU AI Act; (e) Logging and record-keeping obligations in accordance with Art. 26 para. 6 EU AI Act; (f) Transparency towards data subjects in accordance with Art. 50 EU AI Act, including disclosure that they are interacting with an AI system and that an automated result may affect their access to a service. WebPros will only deploy Identity Verification Solutions provided by vendors who fulfil the obligations of AI providers under the EU AI Act, including registration in the EU AI Act database where applicable, and who maintain an up-to-date technical documentation and conformity assessment in accordance with Arts. 11, 16, and 43 EU AI Act.

Third-Party Processor and International Transfers

Identity Verification Solution providers act as data processors on behalf of WebPros pursuant to a Data Processing Agreement in accordance with Art. 28 GDPR. Such agreements require the processor to: (i) process personal data only for the purpose of delivering the verification service; (ii) implement appropriate technical and organizational measures to protect personal data, in particular biometric data; (iii) refrain from using any personal data to train, improve, or develop AI models; (iv) delete or return all personal data upon completion of the verification process or termination of the engagement; and (v) comply with applicable data protection law, including the GDPR and the EU AI Act. Where the Identity Verification Solution provider

is located outside the EU/EEA, transfers are governed by the mechanisms described in the “Third Country Transfer” section of this Policy, in particular standard contractual clauses pursuant to Art. 46 GDPR or, where available, an adequacy decision pursuant to Art. 45 GDPR. Currently, identity verification services may be provided by UAB iDenfy, registered in Lithuania (EU), which as an EU-based processor does not require a separate transfer mechanism. WebPros reserves the right to change or add Identity Verification Solution providers, provided the required safeguards described in this section are fulfilled. Any change will be reflected in the WebPros list of sub-processors, available at webpros.com/legal/.

Retention and Deletion

Biometric data and raw identity document images processed through Identity Verification Solutions are deleted or irreversibly anonymized upon completion of the verification process, unless: (a) applicable law (e.g. AML/KYC regulations) requires retention for a defined period, in which case only the minimum data necessary to fulfil the legal obligation will be retained; or (b) the data subject has given separate explicit consent to a longer retention period. The verification result (i.e. a binary or categorical outcome, without underlying biometric data) may be retained by WebPros for as long as necessary to document compliance with the applicable regulatory obligation or to defend against legal claims, in accordance with the general retention periods described in the “Duration of Data Processing” section of this Policy. Data subjects may request deletion of their verification data at any time by contacting privacy@webpros.com, subject to any overriding legal retention obligations.

Your Rights in the Context of Identity Verification

In addition to your general data subject rights described in the “Your Rights as a Data Subject” section of this Policy, the following specific rights apply in connection with identity verification: (a) Right to withdraw consent at any time prior to completion of the verification, without detriment and without affecting the lawfulness of prior processing; (b) Right to request human review of any automated verification result, by contacting privacy@webpros.com within 30 days of receiving the result; (c) Right to access the personal data processed about you during the verification process, including the verification result and any flags generated; (d) Right to erasure of biometric data immediately upon completion of verification, subject to legal retention obligations; (e) Right to lodge a complaint with a supervisory authority, in particular the competent data protection authority in your country of residence. To exercise any of these rights or to raise concerns about the identity verification process, please contact privacy@webpros.com with the subject line “Identity Verification — Data Subject Request”.

8. Data Retention and Your Rights

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 the “Duration of Data Processing” section of this Policy. Your rights of access, rectification, erasure, restriction, portability, and objection apply equally to data processed through AI Features and are described in the “Your Rights as a Data Subject” section of this Policy. To exercise your rights or raise any AI-related privacy concern, please contact privacy@webpros.com.

F. Duration of Data Processing

We store personal data only as long as it is necessary to achieve the respective purpose or until you revoke your consent.

If there are legal retention obligations - for example, under commercial, tax, or social security law in Switzerland or the EU - the retention of certain data may be required for up to 10 years or longer, regardless of the processing purpose.

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

G. Your rights as a Data Subject

1. Request for Information

Upon request, you can receive information about all personal data we have stored about you at any time, free of charge.

2. Rectification, Erasure, Restriction of Processing (Blocking), Objection

If you no longer agree with the storage of your personal data or if it has become incorrect, we will delete or block 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. You have the right to object, particularly in cases where your data is required for the performance of a task carried out in the public interest or based on our legitimate interest, including profiling based on these grounds. You also have the right to object to data processing for direct marketing purposes.

3. Right to withdraw consent with effect for the future

You can withdraw your consent at any time with effect for the future. Your withdrawal will not affect the lawfulness of the processing up to the time of withdrawal.

4. Data Portability

If data processing is based on a contract, pre-contractual negotiations, consent, or automated procedures, you have the right to data portability. Upon request, we will provide your data in a common, structured, and machine-readable format, so that you can transfer the data to another controller if desired.

5. Restriction of Processing

Data for which we are unable to identify the data subject, for example, if it has been anonymized for analysis purposes, is not covered by the aforementioned rights. Information, deletion, blocking, correction, or transfer to another company may be possible for such data if you provide us with additional information that allows us to identify you.

6. No Automated Decision-making or Profiling

Subject to the exception for Identity Verification Solutions set out hereinabove, Your data is not used by us for automated decisions which have legal consequences for you or significantly affect you in a similar way - as described in Art. 22 GDPR (EU) or Art. 21 DSG (Switzerland).

We also do not conduct so-called profiling. This means that we do not create automated evaluations of your data to analyze or predict personal characteristics such as interests, behavior, or preferences. Should we exceptionally use automated decisions or profiling, we will inform you transparently in advance and obtain your explicit consent where necessary.

7. For WebPros companies domiciled in Switzerland: Inspection of the data collection register

If the data processing is carried out by a WebPros company based in Switzerland, you have the right to inspect the register of data collections at any time. This contains information on which federal bodies and private persons process which kinds of personal data. With the help of the register you can find out who is processing your data and how, and on the basis of this information you can decide which data collection you wish to request information about.

8. Exercising your rights as a Data Subject and right to lodge a complaint

If you have any questions regarding the processing of your personal data, information, rectification, blocking, objection or deletion of data, or if you wish to transfer your data to another enterprise, please contact privacy@WebPros.com.

You also have the option of complaining to a supervisory authority about your rights as a data subject. In the case of a WebPros company based in Switzerland, you have the right to lodge a complaint with the Federal Data Protection and Information Commissioner (FDPIC).

This policy is subject to periodic revisions and may be amended by WebPros from time to time if necessary. Please come back periodically and check for updates.