Who are we?

We are a Ukrainian network startup specializing in the development and provision of VPN services, managed by sole proprietor Merezhiuk Yevhenii, registered at the following address: 03035, Ukraine, Kyiv, Kudryashova Lane, building 10, apartment 8. This Privacy Policy applies to all our services, including the project website https://comfiweb.com/ and our mobile application Comfiweb VPN.

Privacy Policy Contents

This Privacy Policy describes how we handle and protect your personal data and the choices available to you. Additional information on our personal data practices may be provided in product settings, contractual terms, or notices provided prior to or at the time of data collection.

Please refer to our Products Policy describing specifics of personal data processing within our products and services.

This Privacy Policy is intended for you if you are a user of our products and services. If you are a business partner, the privacy notice that applies to you is located here: Business partner policy.

Personal Data We Process

Personal data refers to any information relating to an identified or identifiable individual ("Personal Data").

We may collect data or ask you to provide certain data when you visit our websites, and use our products and services. The sources from which we collect Personal Data include:

- Data collected directly from you or your device relating to an identified or identifiable natural person ("Data Subject"), and may include direct identifiers such as name, postal and email address, phone number, and online or indirect identifiers such as login account, login password, marketing preferences, social media account, and/or IP address;
- If we link other data with your Personal Data, we will treat that linked data as Personal Data; and
- We may also collect Personal Data from trusted third-party sources such as distributors, resellers, app stores, contact centers, and engage third parties such as marketing, survey, analytics or software suppliers to collect Personal Data to assist us.

We do not process special categories of personal data, such as data concerning health, race, ethnicity or political opinions, or deduce in any way this type of information from data we collect within our products.

We organize the Personal Data we process into these basic categories: Billing Data, Account Data, Product Data and Communications Data.

Account Data

Account Data includes information to set up and customize an account, such as your name, email address and username, and information connected with our services, such as product, license and device information. For some of our products or some of their functions creating an account is necessary. Account Data is also used for customer management and engagement, revenue generation, and evaluation and optimization of operational, sales and business processes.

See below an example of Account Data and what we use it for:

Account data	**What we use it for**
Name	To customize our communications by addressing you by your name
Email address	To send you communications regarding your license and support and to offer our other products and services
Username	To manage your account and facilitate your login into the service
Account usage data (events such as request to end subscription, subscription-related information)	To enable premium features activation, provide tailored life-cycle experience and communication with customer support, suitable product interface content.
Subscription renewal date	To help us validate the period the license is active
Trial User	To add a grace period prior to the paid period of the subscription

An account is also necessary for some features of our Forum. **In the Forum profile**, you have the option to provide additional information within your account such as your name, email address, social media information, birth date, gender, instant messaging information, or website name and address, your physical location, and an avatar or personalized picture. We use Discourse for hosting the Forum.

To register with us or to be able to log in later on our pages or in our products, we offer you, in addition to our own procedure, the option to do this via the services Facebook Connect, Google, and Apple ID. For this purpose, we will redirect you to a page of the corresponding provider. Data from the provider (email, platform ID, optionally name) is then provided to create the account.

The customer account remains valid until you actively delete it in the user administration section of the account. You can also contact our support or DPO in case you would like to delete your account.

Product Data

Product Data includes two sub-categories:

- **Device Data** includes information about the operating system; hardware; city/country location of device; IP address, device error logs; browser; network; applications running on the device, including the Comfiweb products; and
- **Service Data** includes information about product usage and events relating to use of our product by you. This information includes samples, detection details, and files used for malware protection, information concerning URLs of websites, usage statistics (activation, crashes, scans, errors).

Communications Data

If you contact us directly, we collect personal data about you, including identifiers, such as your name, email address, phone number, the contents of any message or attachments that you may send or communicate to us, and any other information you choose to provide. We may retain and review audio, electronic, visual, or similar information, such as audio call and chat recordings and/or the contents of the messages as required/permitted by law and our recording and information management policies. We will also collect identifiers from you, such as your email address and phone number, when you sign up to receive product updates, offers, and other promotional information or messages from us. When we send you emails, we may track whether you open them to learn how to deliver a better customer experience and improve our services.

Why We Process Your Personal Data

We use your Personal Data for the following purposes and on the following grounds:

On the basis of fulfilling our contract with you or entering into a contract with you on your request, in order to:

- To process purchase of our products or services from us, our partners or our trusted third-party service providers' online stores and to bill for products and features purchased;
- To provision the download, activation, and performance of the product or service;
- To keep our products or services up-to-date, safe and free of errors, including implementation of new product features and versions;
- To verify your identity and entitlement to paid products or services, when you contact us for support or access our services;
- To process your purchase transactions;

- To update you on the status of your orders and licences;
- To manage your subscriptions and user accounts; and
- To provide you with technical and customer support. This may include remote access to your device to better solve the issue. For this purpose, we will process the information from your product and device (e.g. crash reports, usage data), your contact details as well as other information you will provide to us (e.g. description of the issue).

On the basis of your consent, in order to:

- To subscribe you to a newsletter or the Comfiweb forum;
- To enable the provision of third-party ads in product messages;
- To enable the provision of personalized ads in support of certain free products;

We will always ask for your consent before any processing which requires it and we will provide you with necessary information through our Consent Policy or otherwise as applicable.

In order to fulfill legal obligations, we process your Personal Data when it is necessary for compliance with a legal tax, accounting, anti-money laundering, legal order, sanction checks or other obligations to which we are subject.

On the basis of our legitimate interest we will use your Personal Data to:

- To communicate about possible security, privacy and performance improvements and products that supplement or improve our purchased products and to optimize the content and delivery of this type of communication;
- To evaluate and to improve the performance and quality of our products, services and websites, develop new products, train our employees and to understand usage trends, and analyze user acquisitions, conversions and campaigns;
- To maintain and develop threat intelligence resources, in particular to be able to detect and block malware;
- To make our systems and applications more secure;
- To maintain the effective performance of our business by ensuring necessary internal administrative and commercial processes (e.g. finances, audit, business intelligence, legal & compliance, fraud check, information security etc.); and
- To establish, exercise, or defend our legal rights.

Your interests are a key part of our decision-making process and have been considered in all of the above-mentioned processing activities. We believe we have achieved a fair balance between privacy and business operations. In any case, you have the right to object, on grounds relating to your particular situation, to those processing operations. For more details please see section Your Privacy Rights.

Security and Threat Intelligence

We process Personal Data to support network and information security efforts. In line with EU data protection law, organizations have a recognized legitimate interest in collecting and processing Personal Data in a proportionate manner for the purposes of ensuring network and information security. This covers the ability of our networks or of our information systems to resist events, attacks or unlawful or malicious actions that could compromise the availability, authenticity, integrity and confidentiality of the data we store or transmit, or the security of the related services offered by, or accessible via those networks and systems.

Moreover, as a member of the security community, we also cooperate with other players across the security landscape, in particular by exchanging threat intelligence resources, and aid in research and development of new security solutions.

The Personal Data we process for the purpose listed above includes, without limitation, network traffic data related to cyber-threats such as:

- Sender email addresses (e.g., of sources of SPAM);
- Recipient email addresses (e.g., of victims of targeted email cyberattacks including phishing);
- Email header detail including addresses and intermediary systems (e.g., as configured by cybercriminals sending malicious email);
- Filenames and execution paths (e.g., of malicious or potentially harmful executable files);
- Samples (e.g., of malicious or potentially harmful executable files);
- Samples behavior (e.g., of malicious or potentially harmful files);
- URLs and associated page titles (e.g., of web pages broadcasting or hosting malicious or otherwise harmful content); and/or
- IP addresses (e.g., of web servers and connected devices involved in the generation, distribution, conveyance, hosting, caching or other storage of cyber-threats such as malicious or otherwise harmful content).

How We Process Your Personal Data

We do our best to disconnect or remove all direct identifiers from the Personal Data that we use:

- For free versions, this disconnection or removal of identifiers begins when the products and services are initially activated. For paid users we keep Billing Data in a separate database and minimize its use for anything other than handling payments and our own financial management activities.
- For both paid and free versions, we continuously monitor for, minimize, disconnect and remove all direct identifiers during the normal performance of the products and services.

Processing of IP Addresses

Your IP address is collected at the time at which your product or service is being provided for the purpose of downloading and installing the products, product authorization, fraud and malware detection and for the purpose of facilitating our billing process. In particular for delivering the content in accordance with your device(s) settings, determining appropriate language settings for communicating with you, troubleshooting issues, and generating appropriate diagnostics reports.

How We Disclose Your Personal Data

We only disclose your Personal Data as described below, within our group of companies, with our partners, with service providers that process data on our behalf and with public authorities, when required by applicable law. Processing is only undertaken for the purposes described in this Privacy Policy and the relevant Products Policy sections. If we disclose your Personal Data, we require its recipients to comply with adequate privacy and confidentiality requirements, and security standards.

Payment processors

In certain cases, we may use a third party payment processor to take payment from you. These third parties are properly regulated and authorized to handle your payment information and are prohibited from using your Personal Data for any other purposes other than arranging these services for us. However, they are independent controllers of your data with their own responsibility.

These are our long-term payment processors:

Payment Processor	**Link to Privacy Policy**	**Location**
Digital River	https://www.digitalriver.com/privacy-policy/	US, Ireland
Nexway	https://www.nexway.com/legal-notice-privacy/	Germany, France, USA
Cleverbridge	https://www.cleverbridge.com/?scope=opprivacy	Germany, USA, Japan, Taiwan, Malta
Paypal (Braintree)	https://www.paypal.com/en/webapps/mpp/ua/privacy-full	US, Ireland
Google Play Store (for mobile apps)	https://policies.google.com/privacy	US, Ireland
Apple Store (for mobile apps)	https://www.apple.com/legal/privacy/	US, Ireland

Your Billing Data is processed by the payment processor from whom you purchased the product. Your data is processed according to the relevant processor's terms and privacy policy.

Public Authorities

In certain instances, it may be necessary for us to disclose your Personal Data to public authorities or as otherwise required by applicable law. No Personal Data will be disclosed to any public authority except in response to:

- A subpoena, warrant or other process issued by a court or other public authority of competent jurisdiction;
- A legal process having the same consequence as a court-issued request for data, in that if we were to refuse to provide such data, it would be in breach of local law, and it or its officers, executives or employees would be subject to liability for failing to honor such legal process;
- Where such disclosure is necessary for us to enforce our legal rights pursuant to applicable law; or
- A request for data with the purpose of identifying and/or preventing credit card fraud.

How We Protect Your Personal Data

We maintain administrative, technical, and physical safeguards for the protection of your Personal Data.

Administrative Safeguards

Access to the Personal Data of our users is limited to authorized personnel who have a legitimate need to know based on their job descriptions, for example, employees who provide technical support to end users, or who service user accounts. In the case of third-party contractors who process personal information on our behalf, similar requirements are imposed. These third parties are contractually bound by confidentiality clauses, even when they leave the company. Where an individual employee no longer requires access, that individual's credentials are revoked.

Technical Safeguards

We store your personal information in our database using the protections described above. In addition, we utilize technical safeguards such as up-to-date firewall protection for an additional layer of security, high-quality anti-virus software, and we regularly update our definitions. Third parties who we hire to provide services and who have access to our users' data are required to adopt appropriate measures if we deem them necessary.

Physical Safeguards

Access to user information in our database by Internet requires using an encrypted VPN, except for email which requires user authentication. Third-party contractors who process Personal Data on our behalf agree to provide reasonable physical safeguards.

Proportionality

We strive to collect no more Personal Data from you than is required by the purpose for which we collect it. This, in turn, helps reduce the total risk of harm should data loss or a breach in security occur: the less data we collect, the smaller the overall risk.

Children's Privacy

We may offer products and services designed specifically to assist you as a parent by providing child online protection features. In such cases, we will only collect and process Personal Data related to any child under the age specified in particular jurisdictions, which you choose to disclose to us or otherwise instruct us to collect and process. Details about this processing is included in our Products Policy. Please refer to the specific applicable notices for this information.

How Long We Store Your Personal Data

We will hold your Personal Data on our systems for the following periods:

- For Billing Data, for as long as we have a legal obligation or for our legitimate interests in establishing legal rights and keeping proper business records. We also keep your Billing data to enable the renewal of your subscriptions;
- For Account Data, for as long as you maintain your account;
- For Product Data, only as long as necessary for the purposes of a particular product or service. We use rolling deletion periods which means we regularly delete collected data in the given periods starting from the collection of that respective data. The rolling deletion periods for Product Data are not longer than six years. You can find specific rolling deletion periods for each of our products and their purposes in our Products Policy. Please note that when you uninstall our product, processing for service provision, in-product messaging, analytics and third-party ads, if applicable, dependent on the installed product shall cease. After the uninstallation, we will continue to process your Product Data for statistical purposes for up to six years. We have measures in place to ensure compliance with data protection laws, including pseudonymization.
- For Communications Data, for as long as necessary to resolve your requests or questions and maintain evidence of such communications to defend our rights and protect our interests. If you receive product updates, offers, and other promotional information or messages, we process the data until you unsubscribe.

Storage of Your Personal Data

The data we collect from you may be stored, with risk-appropriate technical and organizational security measures applied to it, on in-house as well as third-party servers in the Ukraine, in the United States, as well as anywhere we or our trusted service providers and partners operate. In particular, we store some of the data in the Google Cloud Platform operated by Google Cloud

EMEA Ltd. Personal Data originating from the EEA are stored on Google's servers in the EEA, however, such data may be also accessed by Google personnel located outside the EEA. We put in place appropriate safeguards, including Standard Contractual Clauses, to address these cross-border transfers of Personal Data.

In all cases, we follow generally accepted standards and security measures to protect the personal data submitted to us, both during transmission and once we receive it.

Your Privacy Rights

You have the following rights regarding the processing of your Personal Data:

- Right to information - Right to receive information about the processing of your Personal Data, prior to processing as well as during the processing, upon request.
- Right of access - You have the right to receive a copy of your Personal Data.
- Right to rectification - You have the right to seek correction of inaccurate Personal Data.
- Right to erasure ("right to be forgotten") - You have the right to erasure of your Personal Data, but only in specific cases stipulated by law, e.g., if there is no legally recognized title on our part for further processing of your Personal Data (incl. protection of our legitimate interests and rights).
- Right to data portability - The right to receive Personal Data which you have provided and is being processed on the basis of consent or where it is necessary for the purpose of conclusion and performance of a contract, in machine-readable format. This right applies exclusively to Personal Data where processing is carried out by automated means.
- Right to object - Applies to cases of processing carried out in legitimate interest. You have the right to object to such processing, on grounds relating to your particular situation, and we are required to assess the processing in order to ensure compliance with all legally binding rules and applicable regulations. In case of direct marketing, we shall cease processing Personal Data for such purposes after the objection.
- Right to withdraw consent - In the case of processing based on your consent, you can withdraw your consent at any time by using the same method (if technically possible) you used to provide it to us (the exact method will be described in more detail with each consent when you provide it). The withdrawal of consent shall not affect the lawfulness of processing based on your consent before its withdrawal.
- Right to restriction of processing - You have the right to restriction of processing of your Personal Data if: You are contesting the accuracy of your Personal Data, for a period enabling us to verify the accuracy of your Personal Data; the processing is unlawful and you oppose the erasure of the Personal Data and request the restriction of its use instead; we no longer need the Personal Data for the purposes of the processing, but they are required by you for the establishment, exercise or defence of legal claims; or you have objected to processing of your Personal Data, and there is a pending verification whether our legitimate grounds override your interests.

You can submit your requests relating to your data subject rights and access to documentation relating to appropriate safeguards for cross-border transfers through our online forms.

The fulfillment of data subject rights listed above will depend on the category of Personal Data and the processing activity. In all cases, we strive to fulfill your request.

We will action your request within one month of receiving a request from you concerning any one of your rights as a Data Subject. When we are faced with an unusually large number of requests or particularly complicated requests, the time limit may be extended to a maximum of another two months. If we fail to meet these deadlines, we would, of course, prefer that you contact us to resolve the situation informally.

Where requests we receive are unfounded or excessive, in particular because they repeat, we may either: (a) charge a reasonable fee taking into account the administrative costs of providing the information or communication or taking the action requested; or (b) refuse to act on the request.

Identification of an individual may not be necessary for some of our free products to be delivered to you or to function. In this case, we do not and will not maintain, acquire or process additional information solely in order to identify the users of our free products and services.

Consistent with our privacy by design, privacy by default and data minimization practices, we may not be able to identify you in connection with Product Data relating to specific free products and services. However, you can go directly to your product settings and explore the available privacy options.

Categories of collected personal information

You can see all categories of collected personal information listed in the section Personal Data We Process.

Sources from which the personal information is collected

You can find information about the sources of data in the section Personal Data We Process.

Business or commercial purpose for collecting or selling personal information

You can find all purposes of processing your personal information listed in the section Why We Process Your Personal Data.

Categories of third parties with whom the business shares personal information

You can find all categories of recipients of personal information listed in the section How We Disclose Your Personal Data. Comfiweb does not sell (as such term is defined in the California Consumer Privacy Act/California Privacy Rights Act) your personal information we collect without providing a right to opt out or your direct permission. See more about your right to opt out of sale below.

Our products are not targeted at minors under 16 years of age. We therefore have no knowledge of any sale of data concerning them.

How long we store your personal information

You have the right to:

- know what personal information is being collected about you and how it's processed;
- know whether your personal information is sold, shared or disclosed, and to whom;
- request that we correct the personal information we have about you that is incorrect;
- say no to the sale or sharing of your personal information (right to opt out);
- limit the use and disclosure of your sensitive personal information;
- request deletion of your personal information; information will be deleted if no exception applies (including our right to defend our lawful interests);
- access your personal information; specific information shall be provided in a portable and, to the extent technically feasible, in a readily useable format but not more than twice in a 12-month period;
- non-retailation, including the right to receive equal service and price, even if you exercise your privacy rights (also known as the right to non-discrimination).

Under California law, we are required to disclose to consumers the following information upon written request: (1) the categories of personal information that we have disclosed to third parties within the prior year, if that information was subsequently used for the third parties' direct marketing purposes; and (2) the names and addresses of all such third parties to whom such personal information was disclosed for the third parties' direct marketing purposes.

We hereby disclose that we have not disclosed any such personal information regarding any California resident during the one-year period prior to the effective date of this Privacy Policy with the exception of:

- third-party advertising cookies stated in our Cookie Policy.
- third-party ads in products listed in our Consent Policy.Right To Opt Out Of Sale or Sharing

If your personal information is subject to a sale or sharing, you have the right to opt out from that sale or sharing.

For more information on how you can opt out of the sale or sharing of your personal information, please consult our "Do Not Sell or Share My Personal Information" page.

Request Submission

You can submit your requests using contacts indicated below in the Contact Us section. We will verify your request by matching your email address and, if necessary, other information you provide in your request against the email address and other information we have in our system. You can also designate an authorized agent to exercise these rights on your behalf. We may require that you provide the authorized agent with written permission to act on your behalf and that the authorized agent verify their identity directly with us.

Contact Us

To exercise any of your rights, or if you have any other questions or complaints about our use of your Personal Data and its privacy, write our Privacy Team through the most convenient channel below:

We are registered as FOP Merezhiuk Yevhenii and our registered address is 03035, Ukraine, Kyiv, Kudryashova Lane, building 10, apartment 8. This Privacy Policy applies to all our services, including the project website https://comfiweb.com/ and our mobile application Comfiweb VPN.

You can always reach us by email at support@comfiweb.com Please type “PRIVACY REQUEST” in the message line of your email so we can have the appropriate member of the team respond.

If you prefer, you can send paper mail to FOP Merezhiuk Yevhenii - 03035, Ukraine, Kyiv, Kudryashova Lane, building 10, apartment 8. Be sure to write "Attention: PRIVACY" in the address so we know where to direct your correspondence.

Data Protection Officer

As required under the GDPR, we have a data protection officer (DPO) to monitor our compliance with the GDPR, provide advice where requested and cooperate with supervisory authorities. You can contact our data protection officer via dpo@comfiweb.com.

Changes to this Privacy Policy

We reserve the right to revise or modify this Privacy Policy. In addition, we may update this Privacy Policy to reflect changes to our data practices. If we make any material changes we will notify you by email (sent to the e-mail address specified in your account), product notification or by means of a notice on this website prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.