

Nuwave Privacy Policy

Last Updated • 24 November 2025

Protecting Your Privacy - Our Commitment

NUWAVE respects your privacy and is committed to ensuring appropriate protections are in place for your personal data. We seek to comply with all currently applicable legislation regarding the protection, security and confidentiality of personal data. In this Privacy Policy (the “Policy”), we describe how we collect, use, disclose and protect personal data. We also outline the rights you may have in respect of your personal data held by us. The Policy relates to your personal data that we may access through your use of this website and in relation to any contract for goods or services or other commercial relationship we may have with you, or with anyone who provides you with access to any of our products and services (such as your employer) that may collect, store or otherwise process your personal data.

NUWAVE and Your Privacy

Regardless of whether you are our customer, a visitor to one of our various NUWAVE websites, or someone we deal with in our day-to-day business, protecting your privacy is important to us and is a responsibility that we take very seriously.

This Policy applies to the different legal entities comprising the NUWAVE group, each of which may process your personal data. References to “Customer”, “You” or “Your” in this document shall include the Customer, Reseller and their end users. References to “NUWAVE”, “We”, “Our” or “Us” in this Policy refer to the relevant company within the NUWAVE group that is responsible for processing your personal data, as indicated in any contract for products or services you may hold with us.

Additional information on our personal data practices may be provided in contractual agreements, supplemental privacy statements, or notices provided to you prior to or at the time of collection of your personal data. For the purposes of this Policy, any reference to “Services” is a reference to all the products and services offered by NUWAVE, whether available online or offline, and any reference to “Sites” is a reference to any of the NUWAVE websites (including any NUWAVE cloud application websites), whether operated under the banner of NUWAVE or a brand name that we own.

Our use of your personal data is governed by this Policy as it may be updated from time-to-time. The most up to date version of the Policy will always be available at <https://www.nuwave.com/policies/#policies>. Your use of our Sites or Services, and any dispute over privacy, is subject to this Policy and our Terms of Service (which are incorporated by

reference into this Policy) and any written contract for Services between you and us or any person who provides you with access to our Services. Depending upon your interactions with NUWAVE, other terms may also be applicable to you and our use of your personal data.

Personal Data We Collect About You and How We Collect It

Account Information: Contact and related information that allows us to communicate with you. We obtain this information when you order or register to receive any of our Services or information about our Services. We collect or receive information from you when you sign up for our Services, create an online account with us, make a purchase, request details or a call back, submit a technical, customer or billing support request, participate in a contest or survey, provide us with feedback or otherwise contact us. The type of information that we collect depends on your interaction with us, but may include, your name, address, telephone number (business or personal), email address (business or personal), postal/billing address (business or residential), and any other information that you choose to provide or is necessary for us to provide Services to you.

Billing Information related to your commercial and financial relationship with us, such as the services we provide to you, the telephone numbers you call and text, your payment history, your credit history, your credit card numbers, security codes and your service history.

Technical and Usage Information related to the Services we provide to you, including information about how you use our networks, services, products or websites. Some examples include:

- **Equipment Data:** Information that relates to and identifies the equipment on our and your networks that you may use or with which you interface for the Services you are receiving. Information might include equipment type, device identifiers, device status, serial numbers, settings, configuration, and software type.
- **Network Performance and Service Usage:** Information about the operation of the equipment, Services and applications you use on our networks or platform. Examples of this might include: call records including where a call was made from and to as well as its date, time, duration and cost (but excluding the content of the calls); the number of text messages sent and received; voice minutes used; bandwidth used and similar information (though We also collect information like transmission rates and delays, data associated with remote monitoring services and security characteristics, and information about your use of our interconnected voice over internet protocol (VoIP) services (including services purchased offline).
- **Web Browsing:** such as IP addresses, URLs, data transmission rates, and delays. We may also receive information about the pages you visit, the time you spend on them, the links or advertisements you see, click on and follow, the referring URL or the webpage that led you to our Sites, the search terms you enter, how often you open an application, and other similar information. Please see the section “Our Use of Cookies and other Tracking Mechanisms” below for more information on this.

- **Location, direction and journey information:** this will be collected based on any connected device you may use our Services on. It includes your ZIP/postal code and street address, as well as the whereabouts of your device. Location Information is generated when your device communicates with cell towers, Wi-Fi routers or access points and/or with other technologies. Any connected device that you own, or which is otherwise linked to you will generate such information that will then be associated with you.

We may collect the above personal data in the course of providing Services to you or to someone who has provided you with access to our Services. We may obtain this information in a number of ways, for example:

- directly from you: for example, when you make a purchase or provide your details in order to subscribe to our Services, submit a web enquiry or set up an account with us;
- automatically: when personal data is generated through your use of our Services or our Sites; and
- from third party sources: we sometimes collect personal data about you from trusted third parties, in connection with Services that we provide to you or propose to provide to you, where appropriate and to the extent we have a justified basis to do so. These include fraud-prevention agencies, business directories, credit check reference/vetting agencies and connected network providers. Anyone who provides you with access to your Services may also provide us with your personal data in that context.

We may combine the personal data that we receive from such other sources with personal data you give to us and with information we automatically collect about you, for example where we need to run a credit check, and then compile a profile of you based on the credit check data and the personal data you have provided.

HOW DO WE USE THE PERSONAL DATA WE COLLECT?

We set out below some of the ways in which we process personal data:

- to fulfil obligations under contract. This includes providing our Services to you; to communicate with you about your use of our Services; to obtain and process payment from you and to fulfil your orders for Services and any obligations on us relating to those services;
- for the purpose for which you specifically provided the information to us, including, to respond to your inquiries, to provide any information that you request, to address technical support tickets, and to provide customer service support;
- to make our Services and communications more relevant to you, including generating customer profiles, delivering customized content to you, to offer location customization, personalized help and instructions, and to otherwise tailor your experiences while using our Sites or our Services;

- to better understand how customers and other third parties access and use our Sites and Services, both on an aggregated and individualized basis;
- to administer, monitor, improve and customize our Sites and Services, for our internal operations, including troubleshooting, network management and network optimization, research and analytical purposes, so that we can provide our customers with a better customer experience;
- to investigate, prevent or take action regarding illegal activities, fraud, threats to our property or personnel and violations of our Terms of Service and/or applicable law and also to meet our legal and regulatory obligations;
- to notify you about our new product releases and service development, alerts, events, updates prices, terms, special offers and associated campaigns and promotions (including via newsletters). Therefore, we and selected third parties may use your personal data to send you marketing communications about products and services based on your preferences and interest. You have a choice and can object to our use of your personal data for marketing purposes. When we are required by law to do so, we will obtain your consent before using your personal data for marketing purposes. If you do opt out, we will stop sending you marketing communications, but we will continue sending you non-marketing communications that relate to the Services you are using (for example billing information, software/portal update communications, password resets etc);
- if you attend an event, we may process information about you gathered in relation to the event and may share information about your attendance with your company. We may also permit designated event partner or conference sponsors to send you communications related to the event if you have shared your contact information at the event. Please note that sponsors from other companies may directly request information about you at their conference booths or presentations, and their use of your personal data that you provide to them will be subject to their privacy policies;
- to assist us in advertising our products and services in various mediums including, sending promotional emails, advertising our services on third party sites and social media platforms, direct mail, and by telemarketing;
- where we ask you for specific consent to a use of your personal data, we will use it in the ways we explain at the time of obtaining that consent; and
- in any way required by law, regulation or the public interest such as in response to requests or orders by government or law enforcement authorities conducting an investigation or to respond to an emergency. This use may require us to disclose your personal data including contact details and/or information about your usage of our Services to relevant authorities or to block, intercept or otherwise interfere with your use of our Services and any personal data generated by that usage. Achieving a balance between, on the one hand ensuring protections for the privacy and other fundamental human rights that may be exercised through use of our Services and, on the other, the

exercise of lawful investigatory powers for the public good on the other can be complicated. We do not accede to such requests without careful consideration of all the circumstances. Even where we are legally obliged to disclose personal data, we will give careful consideration to the extent to which doing so will infringe on the fundamental rights, including the right to privacy, of any person whose personal data is to be disclosed or intercepted and we take whatever steps are practicable to mitigate and minimize any such infringement.

WHAT IS THE JUSTIFICATION FOR THESE USES?

In the EU, our justification (sometimes referred to as “legitimate” or “lawful basis” legal basis) for processing any particular category of personal data will vary depending on the information itself, our relationship with the subject of the personal data, the Service being provided, the specific legal and regulatory requirements of the country in which the Services are being provided, the personal data processed and many other factors. Subject to modifications in specific countries, the legal bases for our processing are as follows:

In order to communicate adequately with you as a user of our Services and to respond to your requests, we need to process information about you and therefore have a legitimate interest in processing this information to ensure the efficient and effective operation of our business;

In order to engage in transactions with customers, suppliers and business partners, and to process purchases and effect installation of our products and deliver Services, we need to process information about you as necessary to enter into or perform a contract with you;

We process personal data for marketing and sales activities based on your consent, where it is required and so indicated on our sites or at the time your personal data is collected, or further to our legitimate interest to market and promote our products and services;

We rely on our legitimate interests to process personal data and other information in order to analyze, develop, improve and optimize our Sites, products and Services, and to maintain the security and integrity of our Sites, network and systems. We also have a legitimate interest in using your personal data in connection with legal claims, compliance, regulatory and investigative purposes as necessary or because applicable laws (including telecommunications laws), regulations or the public interest require us to, such as to comply with legal processes, law enforcement or regulatory authorities or to assist in the prevention, detection or prosecution of crime or to process an opt-out request.

We have carried out balancing tests for all the data processing we carry out on the basis of our legitimate interests and which we have described above. You can obtain information on any of our balancing tests by contacting us using the details set out in this Policy. In all other countries (except in the EU or in jurisdictions where similar EU type requirements exist), our justification for processing your personal data will be based on your consent and/or acceptance of the Terms of Service and this Policy. In all situations, where you withhold any personal data requested by us, we may not be able to provide you with certain Services or parts of Services or functionality.

Automated decision making and profiling

We reserve the right to use AI (Artificial Intelligence) and non-AI based computational logic to automate our engineering and operations. We have implemented comprehensive set of assurance measures aligned with ISO42001:2023 to ensure that AI use is safe and responsible. AI technology or third-party providers can be utilised to enable and analyse your interactions with us, whether they are verbal or non-verbal.

WHEN DO WE SHARE OR DISCLOSE THE PERSONAL DATA WE COLLECT?

Subject to obtaining your consent as may be required in some jurisdictions, we may share or disclose your personal data as necessary for the purposes described above and as further detailed below:

- **Corporate Affiliates.** We may disclose the personal data we collect from you to our corporate affiliates. Where permitted by law and with your consent where required, our affiliates may use your information for the purposes indicated in this Policy, including to market their products and services to you. In processing your personal data, our affiliates follow practices at least as protective as those described in this Policy.
- **Business, Sales and Marketing Partners.** We may offer some of our Services together with or through third parties who may be system integrators, resellers, solution partners, network partners and affinity organizations. If we do so, we will need to share your personal data with these third parties to assist in providing and marketing that Service to you, as well as to enable the third parties to market their own products and services to you (with your permission, if required). We may also share your personal data with companies that are system integrators, resellers, solution partners, network partners and affinity organizations, and whom we believe might offer products and services of interest to you (again with your permission, if required).
- **Third-Party Service Providers.** We employ other companies and individuals to perform functions that are necessary for the provision of the Services or for any of the purposes described above. Examples include: where permitted, jointly offering a product or service, sending communications, processing payments, assessing credit and compliance risks to give you access to our Services, fraud and financial crime prevention detection and prosecution, analyzing data, providing marketing and sales assistance (including advertising and event management), customer relationship management, providing training, these third parties include; system integrators, resellers, solution partners, network partners, affinity organizations, third party vendors, service providers, contractors or agents, and other carriers or providers that we may disclose personal data to where necessary to provide our Services or fulfil your requests or orders, as well as entities that provide website hosting, service/order fulfilment, customer service, and credit card processing, effecting payments, among others. These third-party service providers have access to personal data needed to perform the functions we have entrusted to them but may not use it for other purposes where they process your personal data on our behalf.

Whenever we share personal data with third parties, we take steps to ensure that third party contracts contain appropriate protections for your personal data.

- **Business Transfers.** If we are acquired by or merge with another company, or if substantially all of our assets are transferred to another company (which may occur as part of bankruptcy proceedings), we may transfer your personal data to the other company. We may also need to disclose your personal data before any such acquisition or merger, for example to our advisers and any prospective purchaser's adviser.
- **Legal Protection and in Response to Legal Process.** We may disclose the personal data we hold about you in order to comply with applicable law, in response to or to pursue judicial proceedings, court orders and in other legal processes. We may also disclose, transfer or share it when we believe in good faith that disclosure is necessary: to protect or enforce our rights; protect your safety or the safety of others; investigate or prevent fraud; to respond to government requests – including from government and national or international law enforcement authorities outside of your country of residence – or for national security, public safety and/or law enforcement purposes. Personal data shall only be disclosed when we in good faith believe that we are obliged to do so in accordance with the law or that there are compelling reasons of public interest for us to do so. This will only be after a careful evaluation of all legal requirements and other relevant considerations, including any infringement on the fundamental rights to privacy or freedom of expression that might be impacted by the disclosure.
- **Sharing Aggregated and De-Identified Information.** We may use your personal data to create aggregated and anonymized information which we may share with third parties. Nobody can identify you from that anonymized information. In other circumstances we may pseudonymize your personal data before sharing it with a third party so that we can re-associate you with the information once it has been processed and returned to us. Whilst the third party will not be able to identify you from the pseudonymized information, we will still be able to. We treat pseudonymized data as though it were personal data and ensure the same level of protection for it when sharing with third parties.

INTERNATIONAL TRANSFER OF PERSONAL DATA

Personal data held by NUWAVE is stored on and processed on computers situated in the United States, United Kingdom, the EEA, and in other jurisdictions. NUWAVE and/or our service providers also process data in some other countries for customer care, account management and service provisioning.

If you are an EEA resident, your personal data held by NUWAVE may be transferred to, and stored at, destinations outside the EEA that may not be subject to equivalent data protection laws, including the United States. When you sign up for service with NUWAVE or inquire about our services, we transfer your information to the United States and other countries as necessary to perform our agreement with you or to respond to an inquiry you make. It may also be processed by staff situated outside the EEA who work for us or for one of our suppliers.

Accordingly, by using our services, you authorize the transfer of your information to the United States, where we are based, and to other locations where we and/or our service providers operate, and to its (and their) storage and use as specified in this Privacy Policy and any applicable terms of service or other agreement between you and NUWAVE. In some cases, NUWAVE may seek specific consent for the use or transfer of your information overseas at the time of collection. If you do not consent, we may be unable to provide you with the services you requested. The United States and other countries where we operate may not have protections for personal information equivalent to those in your home country.

Subject to obtaining your consent as required in some jurisdictions, NUWAVE may transfer personal data across national borders in running our business and delivering the Services. In doing so, your personal data may be transferred to and processed by other NUWAVE entities and/or unrelated third parties outside of the country where you are located or where the personal data was collected.

For relevant jurisdictions only (e.g. Mexico, Russia, China and Argentina): By using the Services, you expressly agree to the transfers of personal data to third countries where this requires your consent.

Data Privacy Framework

NUWAVE 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. NUWAVE 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. NUWAVE has 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, the Principles shall govern. To learn more about the Data Privacy Framework (DPF) program, and to view our certification, please visit [Data privacy framework website](#).

US Entities or US subsidiaries of NUWAVE adhering to the DPF Principles are as follows:

- NuWave Communications, Inc, 8275 S. Eastern Ave, Ste 266, Las Vegas, NV 89123, United States
- iPilot Software, LLC, 8275 S. Eastern Ave, Ste 266, Las Vegas, NV 89123, United States

In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, NUWAVE commits to cooperate and comply respectively with the advice of the panel established by the EU data protection authorities (DPAs) and the UK Information Commissioner's Office (ICO) and the Gibraltar Regulatory Authority (GRA) and the Swiss

Federal Data Protection and Information Commissioner (FDPIC) with regard to unresolved complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF.

The Federal Trade Commission has jurisdiction over NUWAVE's compliance with the EU-U.S. Data Privacy Framework (EU-U.S. DPF) and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF).

NUWAVE may be liable in cases of onward transfers of personal data to third parties.

NUWAVE commits to binding arbitration at the request of the individual to address any complaint that has not been resolved by other recourse and enforcement mechanisms. If you have a complaint, do not hesitate to contact our Privacy Manager at privacy@nuwave.com. We aim to respond to any such comments or complaints within 45 days.

Alternatively, you could contact your home country independent authority set up to uphold information rights in the public interest.

For example, in the UK you can contact the supervisory authority by visiting <https://ico.org.uk/global/contact-us/>.