

Privacy Policy

Our Privacy Policy was updated on 29th April, 2025 and took effect on 29th April, 2025. This Privacy Policy can provide details on how we manage your personal information for our products and services, unless a separate privacy policy is provided for the specific products or service provided by Lumi United Technology Co., Ltd. and its affiliates (Include but not limited to Shenzhen Aqara Software Service Co., Ltd.),(hereinafter referred to as “Lumi Company”, “we”, “us” or “our”).

Please take a moment to familiarize yourself with our privacy practices and let us know if you have any questions.

Your privacy is critically important to us. At Aqara Forum, we have a few fundamental principles:

- We don't ask you for personal information unless we truly need it. (We won't ask you for things like your gender or income level)
- We don't share your personal information with anyone except to comply with the law, develop our products, or protect our rights.
- We don't store personal information on our servers unless required for the ongoing operation of one of our services.

Contact Us: If you have questions about deleting or correcting your personal data please contact our support team: privacy@lumiunited.com

Website Visitors

Like most websites, Aqara Forum collects non-personally-identifying information which web browsers and servers typically make available, such as the browser type, language preference, referring site, and the date and time of each visitor request. Aqara Forum's purpose in collecting non-personally identifying information is to better understand how Aqara Forum's visitors use its website.

Aqara Forum also collects potentially personally-identifying information like Internet Protocol (IP) addresses for logged in users and for users leaving comments on the blog or forums. Aqara Forum only discloses logged in user and commenter IP addresses under the same circumstances that it uses and discloses personally-identifying information as described below.

Gathering of Personally-Identifying Information

Certain visitors to Aqara Forum's websites choose to interact with Aqara Forum in ways that require Aqara Forum to gather personally-identifying information. The amount and type of information that Aqara Forum gathers depends on the nature of the interaction. For example, we ask visitors who create a forum account to provide a username and an email address. In each case, Aqara Forum collects such information only insofar as is necessary or appropriate to fulfill the purpose of the visitor's interaction with Aqara Forum. Aqara Forum does not disclose personally-identifying information other than as described below. And visitors can always refuse to supply personally-identifying information, with the caveat that it may prevent them from engaging in certain website-related activities.

Aggregated Statistics

Aqara Forum may collect statistics about the behavior of visitors to its website. For instance, Aqara Forum may monitor the most popular topic. Aqara Forum may display this information publicly or provide it to others. However, Aqara Forum does not disclose personally-identifying information other than as described below.

Information We Collect from Other Sources

With your authorization, we may also obtain information about you from other sources. For example, if you create or log into your Aqara Forum Community account through a social media service (like Facebook or Google) or if you connect your account to a social media service, we will receive information from that service (such as your username, basic profile information, and friends list) via the authorization procedures used by that service. The information we receive depends on which services you authorize and any options that are available.

Protection of Certain Personally-Identifying Information

Aqara Forum discloses potentially personally-identifying and personally-identifying information only to its employees, contractors and affiliated organizations that (i) need to know that information in order to process it on Aqara Forum's behalf or to provide services available at Aqara Forum's websites, and (ii) that have agreed not to disclose it to others. Some of those employees, contractors and affiliated organizations may be located outside of your home country; by using Aqara Forum's websites, you consent to the transfer of such information to them. Aqara Forum will not rent or sell potentially personally-identifying and personally-identifying information to anyone. Other than to its employees, contractors and affiliated organizations, as described above, Aqara Forum discloses potentially personally-identifying and personally-identifying information only in response to a subpoena, court order or other governmental request, or when Aqara Forum believes in good faith that disclosure is reasonably necessary to protect the property or rights of Aqara Forum, third parties or the public at large. If you are a registered user of an Aqara Forum website and have supplied your email address, Aqara Forum may occasionally send you an email to tell you about new features, solicit your feedback, or just keep you up to date with what's going on with Aqara Forum and our products. We primarily use our various product blogs to communicate this type of information, so we expect to keep this type of email to a minimum.

If you send us a request (for example via a support email or via one of our feedback mechanisms), we reserve the right to publish it in order to help us clarify or respond to your request or to help us support other users. Aqara Forum takes all measures reasonably necessary to protect against the unauthorized access, use, alteration or destruction of potentially personally-identifying and personally-identifying information.

Cookies

Aqara and its third-party partners and providers use cookies and similar technologies to automatically collect certain personal data when you visit or interact with our sites and services to enhance navigation, analyze trends, administer the sites, track users' movements around the sites, gather demographic information about our user base as a whole, and assist with our marketing efforts and customer service. You can control the use of cookies at the individual browser level, but if you choose to disable cookies, it may limit your use of certain features or functions on our sites and services.

We honor the Global Privacy Control (GPC) signal. If your browser sends a GPC request, we will automatically opt you out of cookie-based sales and targeted advertising, consistent with your settings.

You may also be able to utilize third-party tools and features to further restrict our use of cookies and similar technologies. For example, cookies may generally be disabled or removed by tools available as part of most commercial browsers, and in some instances blocked in the future by selecting certain settings. Browsers offer different functionalities and options, so you may need to set them separately.

Protection of Certain Personally Identifying Information

Aqara Forum discloses potentially personally identifying information only to its employees, contractors and affiliated organizations that (i) need to know that information to process it on our behalf, and (ii) that have agreed not to disclose it to others. **Where personal data is transferred from the European Economic Area (EEA) to third countries, we ensure such transfers are based on appropriate safeguards, including the use of European Commission-approved Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs), to protect your data in accordance with GDPR requirements.** Some recipients may be located outside your home country; by using our websites, you consent to such transfers under these safeguards.

Aqara will not rent or sell personal data to anyone. We disclose personal data only in response to legal requests or to protect rights as described below.

Data Retention

We have implemented processes designed to ensure that your personal data is only processed for the minimum period necessary for the purposes set out in this privacy notice.

The criteria for determining the duration for which we will retain your personal data is as follows:

- (1) We will retain personal data in a form that permits identification only for as long as:
 - (a) we maintain an ongoing relationship with you (e.g., where you are a user of our services, or you are lawfully included in our mailing list and have not unsubscribed); or
 - (b) your personal data is necessary in connection with the lawful purposes set out in this privacy notice, for which we have a valid legal basis (e.g., where your personal data is included in a contract between you and us, and we have a legitimate interest in processing the personal data for the purposes of operating our business and fulfilling our obligations under that contract; or where we have a legal obligation to retain your personal data),
- (2) the duration of:
 - (a) any applicable limitation period under applicable law (i.e., either any statutory retention periods as required by the law of the applicable region (e.g., the European Union or a member state of the EEA), or any period during which any person could bring a legal claim against us in connection with your personal data, or to which your personal data is relevant); and
 - (b) an additional two (2) month period following the end of such applicable limitation period (so that, if a person brings a claim at the end of the limitation period, we are still afforded a reasonable amount of time in which to identify any personal data that is relevant to that claim),
- (3) in addition, if any relevant legal claims are brought, we continue to process personal data for such additional periods as are necessary in connection with that claim.

During the periods noted in paragraphs (2)(a) and (2)(b) above, we will restrict our processing of your personal data to storage of, and maintaining the security of, that data, except to the extent that the data needs to be reviewed in connection with any legal claim, or any obligation under applicable law.

We maintain a record of processing activities as required by applicable laws, documenting details of data processing purposes, categories of data, recipients, retention periods, and security measures. This record helps ensure transparency and compliance with our data protection obligations.

Once the periods in paragraphs (1), (2) and (3) above, each to the extent applicable, have concluded, we will either:

permanently delete or destroy the relevant personal data; or anonymize or deidentify the relevant personal data.

Your Privacy Rights

You have rights and choices when it comes to your personal data. You may be afforded certain rights under applicable laws, which may include the right to access, delete, update, or rectify your data, to be informed of the processing of your data, to file complaints with authorities, and potentially other rights:

- the right not to provide your personal data to us (however, please note that we may be unable to provide you with the full benefit of our services, if you do not provide us with your personal data – e.g., we might not be able to process your requests without the necessary details);
- the right to request access to, or copies of, your relevant personal data, together with additional information, such as information regarding the nature, processing and disclosure of said relevant personal data;
- the right to request rectification of any inaccuracies or incompleteness in your relevant personal data;
- the right to request, on legitimate grounds, restricting the processing of your relevant personal data (limiting the purposes for which we process your personal data);
- the right to have certain relevant personal data transferred to another controller, in a structured, commonly used and machine-readable format, to the extent applicable;
- the right to request the deletion or removal of your relevant personal data where there is no other legal basis for us to keep using it. Please note that we may not be able to immediately remove the information from the backup system due to applicable laws and regulations or technological limitations. If this is the case, we will isolate your relevant personal data from any further processing until the backup can be deleted or be anonymized / deidentified.
- where we process your relevant personal data on the basis of your consent, the right to withdraw that consent at any time (noting that such withdrawal does not affect the lawfulness of any processing performed prior to the date on which we receive notice of such withdrawal).
- Under the GDPR, you may also have the following additional rights regarding the processing of your relevant personal data:
 - the right to object, on grounds relating to your particular situation, to the processing of your relevant personal data by us or on our behalf, where such processing is based on Articles 6(1)(e) (public interest) or 6(1)(f) (legitimate interests) of the GDPR;
 - the right to object to the processing of your relevant personal data by us or on our behalf for direct marketing purposes.

This does not affect your statutory rights.

To exercise one or more of these rights, or to ask a question about these rights or any other provision of this Privacy Notice, or about our processing of your personal data. Please note that:

- in some cases it will be necessary to provide evidence of your identity before we can give effect to these rights; and
- where your request requires the establishment of additional facts (e.g., a determination of whether any processing is non-compliant with applicable law) we will investigate your request within a reasonable amount of time, before deciding what action to take.

To exercise your rights (e.g., access, deletion, correction), you may:

Verification Requirements: For security, we may request proof of identity (e.g., copy of government ID) or account authentication.

Response Time: We aim to respond to requests within 20 business days (or as required by your jurisdiction's law, e.g., 1 month under GDPR, 45 days under California law).

EU Specific Rights:

Under GDPR, you may object to processing based on legitimate interests (Article 6(1)(f)) or public interest (Article 6(1)(e)).

You have the right to lodge a complaint with a data protection authority in your EU member state.

However, we encourage you to first contact us so that we can solve any concerns you may have together.

DATA PROTECTION OFFICER & REPRESENTATIVE

You can contact our Data Protection Officer (DPO) at:

Lumi United Technology Co., Ltd

c/o Data Protection Officer

Room 801-804, Building 1, Chongwen Park, Nanshan iPark, No. 3370, Liuxian Avenue, Fuguang Community, Taoyuan Residential District, Nanshan, Shenzhen, China

Email: privacy@lumiunited.com

We also appointed a representative in the EU according to Art 27 GDPR. You can contact our representative at:

GDPR-Rep.eu

Maetzler Rechtsanwalts GmbH & Co KG

c/o Lumi United Technology Co., Ltd

Schellinggasse 3/10,1010 Vienna, Austria

Please add the following subject to all correspondence: "GDPR-REP ID: 13345230"

<https://gdpr-rep.eu/q/13345230>

Supplemental Terms – Jurisdiction-Specific

UNITED STATES

These following disclosures supplement the information contained in the main body of our privacy policy by providing additional information about our personal data processing practices relating to individual residents of certain states in the United States, including the states of California, Nevada, Colorado, Connecticut, Montana, Oregon, Texas, Utah, or Virginia. For a detailed description of how we collect, use, disclose, and otherwise process personal data, please read the main body of our privacy policy.

California Residents (CPRA/CCPA)

- Sensitive Personal Data Rights: You may direct us to limit the use of sensitive personal data (e.g., biometrics, health data) by submitting a request via privacy@lumiunited.com. We will not process sensitive data beyond the purposes for which it was collected, unless you consent or law requires it.
- Opt-Out of Sales/Targeted Advertising: California residents may opt out of the sale of personal data or its use for targeted advertising by:
 - Adjusting cookie settings via “Cookie Settings” in our website footer;
 - Submitting a written request to privacy@lumiunited.com with “California Opt-Out” in the subject line.

Nevada Residents

Definition of “Sale”: Under Nevada law, we consider a “sale” as the exchange of personal data for monetary value. You may direct us to not sell your personal data by emailing privacy@lumiunited.com with “Nevada Sale Opt-Out” in the subject line.

Virginia/VCDPA & Colorado/CPA Residents

- Transparent Processing Purposes: For each category of personal data (e.g., IP addresses, device info), we process it only for the following specific purposes:
- Identifiers (name, email): Account management, service delivery, and communication.
- Internet/Network Info: Security monitoring, traffic analysis, and technical support.
- Automated Decision-Making: While we do not engage in automated decisions with legal or significant impacts, we provide transparency about any algorithmic processes upon request.

Collection and Use of Personal Data

Personal Data

As described in more detail above, we collect, and have collected in the preceding 12 months, the following categories of personal data:

- Identifiers, such as first and last name, preferred name, phone number, email address, user ID, and online identifiers.
- Internet / network information, such as the device type, manufacturer, and model, operating system, IP address, browser type, internet service provider, and unique identifiers associated with you, your device, or your network.
- Other personal data, such as your communication preferences, entertainment preferences, home configuration (for our home-related services), and any other personal data you choose to share in custom messages sent through the forms, email addresses, or other contact information we make available to customers.
- Inferences, including consumer preferences, predispositions, and characteristics.

As described above, we collect this personal data directly from you, automatically when you interact with our sites, applications, products, or other services, from third parties, and from public third-party platforms such as social media websites.

Sensitive Personal Data

The following personal data elements we collect or are otherwise processed in connection with our sites, applications, products or services may be classified as “sensitive” under certain privacy laws (“Sensitive Personal Data”):

- Account credentials.
- Payment card information (collected and processed solely by our third-party payment providers; Aqara does not have access to this data).

We only use or disclose sensitive personal data where reasonably necessary and proportionate, and where permitted by law, for the purposes of performing services you have requested, verifying and improving the services we provide, detecting security incidents, fraud and other illegal actions, ensuring the physical safety of natural persons, performing services on behalf of the business, or short-term transient use. We only collect and process sensitive personal data without the purpose of inferring characteristics about the relevant individual, and we do not sell sensitive personal data or process or otherwise share sensitive personal data for the purpose of targeted advertising (as further described below).

However, depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to limit, or withdraw your consent for, our processing of

sensitive personal data (as described in the Your Additional U.S. Privacy Choices section below).

We Keep Your Information Safe and Secure

All Aqara products are built with strong security features that continuously protect your information. The insights we gain from maintaining our services help us detect and automatically block security threats from ever reaching you. If we do detect something risky that we think you should know about, we'll notify you and help guide you through the steps to stay better protected.

We work hard to protect you and Aqara from unauthorized access, alteration, disclosure, or destruction of the information we hold, including:

- We use encryption to keep your data private while in transit
- We offer a range of security features, like Safe Browsing, Security Checkup, and 2 Step Verification to help you protect your account
- We review our information collection, storage, and processing practices, including physical security measures, to prevent unauthorized access to our systems
- We restrict accessing personal information to Aqara employees, contractors, and agents who need that information in order to process it. Anyone with this access is subject to strict contractual confidentiality obligations .

Personal Data Disclosures, Sales, and Targeted Advertising

We may disclose the categories of personal data above to the following categories of third parties: the entities that make up the Aqara group, Processors, ad networks and advertising partners, business and marketing partners, third-party providers with services integrating with our services, individuals you choose to share personal data with, and certain third parties where you have provided consent or where otherwise required or permitted by law. Please be aware that we will not transfer your sensitive personal data to any third parties, including advertising platforms, data brokers, or information resellers, for purposes other than providing or improving the use case or features of our sites, applications, products, or services, without your consent.

Our disclosure or making available of identifiers, customer records, commercial information, internet / network information, and inferences to ad networks and advertising partners may qualify as the sale of personal data or the sharing or processing of personal data for the purpose of displaying advertisements that are selected based on personal data obtained or inferred over time from an individual's activities across businesses or distinctly-branded websites, applications, or other services (otherwise known as "targeted advertising" or "cross-context behavioral advertising") under certain privacy laws. Depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to limit or opt-out of the sale of personal data or the processing of personal data for purposes of targeted advertising (as described in the Your Additional U.S. Privacy Choices section below). Please note we do not sell the personal data of individuals we know to be less than 16 years

of age or share such information for targeted advertising purposes. In addition, we do not sell sensitive personal data, and we do not process or otherwise share sensitive personal data for the purpose of targeted advertising.

Automated Decision-Making and Profiling: We do not conduct automated processing of personal data for the purposes of evaluating, analyzing, or predicting an individual's personal aspects in furtherance of decisions that produce legal or similarly significant effects. As a result, we do not provide a right to exercise control over such forms of automated decision-making and profiling. With additional U.S. privacy choices depending on your state of residency and subject to certain legal limitations and exceptions, you may be able to exercise some or all of the following rights:

- **Right to Know.** The right to confirm whether we are processing personal data about you and, under California and Oregon law only, to obtain certain personalized details about the personal data we have collected about you, including:
 - The categories of personal data collected;
 - The categories of sources of the personal data
 - The purposes for which the personal data was collected;
 - The categories of personal data disclosed to third parties (if any), and the categories of recipients to whom this personal data was disclosed to (or, for Oregon residents only, a list of the specific third parties to whom personal data have been disclosed);
 - The categories of personal data shared for targeted advertising purposes (if any), and the categories of recipients to whom the personal data was disclosed for these purposes; and
 - The categories of personal data sold (if any) and the categories of third parties to whom the personal data was sold to.
- **Right to Access & Portability:** The right to obtain access to the personal data we have collected about you and, where required by law, the right to obtain a copy of the personal data in a portable and, to the extent technically feasible, readily usable format that allows you to transmit the data to another entity without hindrance.
- **Right to Correction:** The right to correct inaccuracies in your personal data, taking into account the nature of the personal data and the purposes of the processing of the personal data.
- **Right to Control Over Sensitive Personal Data:** The right to exercise control over our collection and processing of certain sensitive personal data.
- **Right to Opt-Out of Targeted Advertising:** The right to direct us not to use or share personal data for certain targeted advertising purposes.
- **Right to Opt-Out of Sales:** The right to direct us not to sell personal data to third parties.

- **Right to Deletion:** The right to have us delete personal data we maintain about you (subject to certain exceptions).

Depending on your state of residency, you may also have the right to not receive retaliatory or discriminatory treatment in connection with a request to exercise the above rights.

However, the exercise of the rights described above may result in a different price, rate or quality level of product or service where that difference is reasonably related to the impact the right has on our relationship or is otherwise permitted by law.

Submitting Privacy Rights Requests

Please submit a request specifying the right you wish to exercise by:

Sending us an email at the following address: privacy@lumiunited.com.

To exercise your right to opt-out as it relates to the use of cookies and similar technologies that involve the sale of personal data or the use of personal data for targeted advertising purposes, please click the “Cookie Settings” link in the footer of the website and adjust your preferences accordingly. If you are visiting our sites with the Global Privacy Control enabled, any cookies that constitute sales or are used for targeted advertising should already be turned off automatically in our cookie preference manager. Please note this opt-out tool is website, device and browser specific, so you will need to change your preferences on each device and browser you use to interact with the specific website you are visiting.

Before processing your request to exercise certain rights (including the Right to Know, Access & Portability, Correction, and Deletion), we will need to verify your identity and confirm you are a resident of a state that offers the requested right(s). In order to verify your identity, we will generally either require the successful authentication of your account, or the matching of sufficient information you provide us to the information we maintain about you in our systems. As a result, we require requests submitted through our online form and email address to include the requester’s name and email address, their relationship with Aqara, the brands relevant to the request, and the data subject’s email address, state/ country/ zip and any comments relating to the request.

In certain circumstances, we may decline or limit your request, particularly where we are unable to verify your identity or locate your information in our systems, or where you are not a resident of one of the eligible states.

Submitting Authorized Agent Requests

In certain circumstances, you are permitted to use an authorized agent to submit requests on your behalf through the designated methods set forth above where we can verify the authorized agent’s authority to act on your behalf. In order to verify the authorized agent’s authority, we generally require evidence of either (i) a valid power of attorney or (ii) a signed letter containing your name and contact information, the name and contact information of the authorized agent, and a statement of authorization for the request. Depending on the evidence provided and your state of residency, we may still need to separately reach out to you to confirm the authorized agent has permission to act on your behalf and to verify your identity in connection with the request.

Appealing Privacy Rights Decisions

Depending on your state of residency, you may be able to appeal a decision we have made in connection with your privacy rights request. All appeal requests should be submitted by replying to the communication resolving your original request.

Third-Party Service Providers

We engage third-party service providers (e.g., payment processors, cloud hosts) to assist in operating our services. **All third parties are contractually bound to:**

- Process data only as instructed by us;
- Implement appropriate technical and organizational measures to protect data security (e.g., encryption, access controls) ;
- Subcontract only with our written approval and ensure subcontractors adhere to the same obligations.

Business Transfers

If Aqara Forum, or substantially all of its assets, were acquired, or in the unlikely event that Aqara Forum goes out of business or enters bankruptcy, user information would be one of the assets that is transferred or acquired by a third party. You acknowledge that such transfers may occur, and that any acquirer of Aqara Forum may continue to use your personal information as set forth in this policy.

In the event of a business transfer (e.g., acquisition, bankruptcy), any acquirer of our assets will be contractually required to adhere to this privacy policy and safeguard your personal data in compliance with applicable laws.

MISCELLANEOUS

MINORS

Our services are intended for individuals **13 years of age or older** (consistent with COPPA for U.S. residents under 13). **For users under 16 in the EU/EEA**, parental consent is required to process personal data. If a parent believes a minor has provided data without consent, please contact us to delete the data and unsubscribe the minor from our services.

Lumi Company does not seek or intend to seek to receive any personal data from minors. Should a parent or guardian have reasons to believe that a minor has provided Lumi Company with personal data without their prior consent, please contact us to ensure that the personal data is removed and the minor unsubscribes from any of the applicable Lumi Company's services.

UPDATES TO THE PRIVACY POLICY

We keep our privacy policy under regular review and may update this privacy policy to reflect changes to our information practices. If we make material changes to our privacy policy, we will notify you by email (sent to the e-mail address specified in your account) and post the changes on all the Lumi Company's websites or through our software, so that you may be aware of the information we collect and how we use it. Such changes to our privacy policy shall apply from the effective date as set out in the notice or on the website.

We define a “material change” as any update that affects:

- The types of personal data we collect;
- The purposes for which we use data;
- Our data sharing practices with third parties;
- Your rights or choices regarding your data.

Historical versions of the policy are available upon request to privacy@lumiunited.com.

CONTACT US

If you have any comments or questions about this privacy policy or any questions relating to Lumi Company’s collection, use or disclosure of your personal information, please contact us at the address below referencing "Privacy Policy":

Lumi United Technology Co., Ltd

Room 801-804, Building 1, Chongwen Park, Nanshan iPark, No. 3370, Liuxian Avenue,
Fuguang Community, Taoyuan Residential District, Nanshan District, Shenzhen, China

Email: privacy@lumiunited.com

Thank you for taking the time to understand our privacy policy!