

## LINKSYS CLOUD MANAGER PRIVACY NOTICE

To help you find information quickly on any particular question you might have, we have set out an index below. Just click on the question or issue you are interested in and you will be taken to the relevant section:

<b>What types of personal data does Linksys collect about you when you use the Service and what is the purpose of collection?</b> .....	<b>1</b>
<b>With whom might Linksys share my personal data?</b> .....	<b>4</b>
<b>Where might Linksys transfer my personal data?</b> .....	<b>5</b>
<b>How does Linksys aim to keep my personal data secure?</b> .....	<b>5</b>
<b>How long will Linksys keep my personal data?</b> .....	<b>6</b>
<b>What rights do I have in respect of my personal data?</b> .....	<b>6</b>
<b>Information for California Residents</b> .....	<b>8</b>
<b>How do I contact you about my privacy rights?</b> .....	<b>8</b>
<b>Updates to this Privacy Notice</b> .....	<b>8</b>

Please read this Linksys Cloud Manager Privacy Notice (“Privacy Notice”) carefully before completing the registration process and/or using the Linksys Cloud Manager service (“Service”). This Privacy Notice is provided as a separate notice of the Linksys Cloud Manager Terms of Service (the “Agreement”). In this Privacy Notice, Belkin International, Inc. (together with its affiliates, “Linksys”, “we” or “us”) provides details of how information is handled when you use the Service, including any apps (“Apps”) that facilitate use of the Service. The purpose of this Privacy Notice is to give you information about how Linksys collects, processes, stores and otherwise uses information about you, and your rights in relation to that information. If you are visually impaired, you may access this notice through your browser’s audio reader.

Please ensure you share this Privacy Notice with anybody else (e.g. in your organization and/or on your network) using the Service.

In this Notice you will see references to “GDPR” - that refer to the European Union (“EU”) General Data Protection Regulation. If you are in the European Economic Area (“EEA”), the GDPR governs your rights in relation to your personal data and how organizations should protect it. You may also see references to “CCPA” – that refers to the California Consumer Privacy Act. If you are in California, the CCPA governs your rights in relation to your personal data and how organizations should protect it.

This Privacy Notice contains important information about your rights and obligations, as well as limitations and exclusions that may apply to you.

We process the data that you enter or upload to the Service in accordance with this Privacy Notice and the Agreement. Certain data collected from the Service, or that you provide or make accessible as part of your use of the Service, is necessary for the essential use and functionality of the Service or to provide associated services as set forth in this Privacy Notice. These are labeled as “Required Data” under the categories of personal data below. Accordingly, you may not be able to opt-out of certain data collection practices without terminating your use of the Service.

### **What types of personal data does Linksys collect about you when you use the Service and what is the purpose of collection?**

“Personal data” or “personal information” means any information relating to you or relating to another identified or identifiable natural person, including where such information is defined under the data

protection laws applicable in the jurisdiction in which such person resides to be "personal data" or "personal information" or any other similar term and includes, without limitation, "personal data" as defined in the GDPR in respect of individuals resident in the EEA, "personal information" as defined in the CCPA in respect of individuals resident in California, United States, or "personal information" as defined in the *Privacy Act 1988 (Cth)* in respect of individuals resident in Australia.

Anonymized Information. When information is anonymized, personal data is removed from collected data and the remaining portion of the data is repurposed for internal or external use, such as to determine how many users of a particular router include an Internet-enabled television in a home network environment. Anonymized information cannot be used to identify you.

*Children's Personal Data.* The Service and Linksys products are not directed to, nor does Linksys knowingly collect personal data from children under the age of 16. If you believe we might have inadvertently collected personal data from or about a child under the age of 16, please contact us [here](#) and we will delete it. We do not sell the personal information of minors under 16 years of age.

The following provides examples of the types of information we collect about you and how we use that information.

Context	Types of Data	Primary Purposes for Collection and Use of Data
Account Registration/ Authentication Data	<p>We collect your email address and password when you provide them to us when creating a Linksys Cloud Manager account. Your password is only stored in hashed form. We also collect information when you are logged into your account, including your IP address, MAC address and the serial number of each access point.</p> <p>Authentication Data is Required Data.</p>	<p>We have a legitimate interest in providing account related functionalities to our users, including securely authenticating your account with us. Account information can be used to save your preferences and transaction history; to notify you about firmware updates, service downtimes, security issues, new features and other communications about the Service; and to provide you with more efficient customer support. We also use account information to notify you about changes to the Agreement to perform our contract with you.</p> <p>IP address is collected so that we know which Internet server each access point is connected to and which of your end users devices are using which access point. We have a legitimate interest in making sure the Service is working properly and troubleshooting problems with connectivity that our users may be having.</p> <p>The MAC address and serial number of each access point are collected because we have a legitimate interest in making sure that your access points are mapped properly so that you (and only you) can see them on the Cloud Manager map. We also have a legitimate interest in making you're your access points are working properly and troubleshooting problems that a particular access point may have with the Service.</p>

Optional Data about your small and medium business (SMB) network	You have the option to provide us with the following information about your SMB network: name of contact person, phone number, address or location of access points in your network, and name of access points.	We have a legitimate interest in providing you with an efficient and robust Service, so we have given users the option to provide the name of a contact person and phone number so that we can quickly contact someone at your company for customer support purposes and to make sure that notifications about technical notes and alerts, security issues, firmware updates and other communications relating to the Service are going to the right person in your organization.  We also have a legitimate interest in providing you with the most accurate Cloud Manager map, so collecting the address or location of access points and names of access points allows you to more easily see your access points on the Cloud Manager map. This helps you to identify which access points are connected to the Internet and for you to troubleshoot connectivity issues on your own.
Customer Support	If you report a problem or contact us for support, we will collect your name, phone number, email address and information about your SMB network and devices connected to your SMB network.  If you submit a Return Materials Authorization, we will collect your physical address and credit card number.	We use your information to perform our contract to provide you with products or services and to honor product warranties. We also have a legitimate interest in providing support to our customers and fixing issues that they bring to our attention, as well as developing new products and improving current products based on your feedback.
Service Interactions/ Usage Data	We use technology to monitor how you interact with the Service. This may include network statistics and configurations, what browser you use, when the Service is accessed by you, log in/ log off data.  Usage Data is Required Data.	We have a legitimate interest in understanding how you interact with our Service to better improve it, to ensure that content is presented in the most effective manner, and to troubleshoot issues to understand your preferences and interests in order to select offerings that you might find most useful. If you consent, user log and access data may also be used during customer support to troubleshoot issues with your use of the Service. We also have a legitimate interest in detecting and preventing fraud and ensuring that your experience on our Service is as secure as possible.

In addition to the information that we collect from you directly, we may also receive information about you from other sources, including third parties, business partners, our affiliates, or publicly available sources.

If you choose not to provide your personal data to us for the purposes set out in this Privacy Notice, or if we do not or are unable to collect the personal data we require, we may not be able to provide you with requested information, products or services, or to effectively conduct our relationship with you.

For Optional Data about your SMB network, you are entitled to let us know at any time if you do not wish us to continue to process this information. This may mean that certain aspects of the Service will not be available to you, but you will still be able to use other aspects of the Service. For example, if you tell us to delete data relating to a contact person's name, email and/or phone number, you will still be able to use the Service, but we may not have a means to notify you of improvements to the Service or upcoming firmware updates. Similarly, if you tell us to delete location of access points, we can delete specific data, but without general location data, you would not be able to locate your access points on the Cloud Manager map.

We may otherwise collect, use or disclose your personal data where the collection, use or disclosure is:

- in accordance with this Privacy Notice or any agreement you enter into with us; or
- required or authorised by applicable law.

## **With whom might Linksys share my personal data?**

Linksys does not rent or sell personal data.

Linksys is part of the Belkin group of companies ("Belkin Group"). In addition, the Belkin Group is owned by Foxconn Interconnect Technology, a Hon Hai company, which includes companies in the Foxconn group of companies ("FIT Group"). Linksys may transfer personal data to third parties, including to entities within and outside the Belkin Group and FIT Group located in any jurisdictions where Belkin Group entities and FIT Group entities are located, for the processing purposes set forth in this Privacy Notice, as follows:

- **To companies within the Belkin Group and FIT Group.**
- **To general service providers.** As necessary to provide the Service to you. Below is a non-exhaustive list of service providers that we may share your data with, including the related processing purposes for which it is disclosed:
  - o Tanaza S.p.A. – We provide Authentication Data and Usage Data to Tanaza to assist us with authentication, troubleshooting connectivity and making sure the Service is working properly and improving Linksys products.
- **To customer support service providers.** As necessary to provide you with customer support if you contact our customer support team:
  - o Concentrix
  - o CSS
  - o Sutherland
  - o Salesforce
- **To regulators, authorities, and other third parties.** As necessary to comply with the law or legal process, personal information may be transferred to regulators, courts, and other authorities (e.g., tax and law enforcement authorities), independent external advisors (e.g., auditors), and internal compliance and investigation teams (including external advisers appointed to conduct internal investigations).
- **To acquiring entities.** Your personal data may be transferred to third parties involved in a reorganisation, restructuring, merger, acquisition or transfer of assets of the Linksys business in

whole or in part including the successor entity provided that the receiving party agrees to treat your personal data in a manner consistent with this Privacy Notice.

- **With your consent.** We may ask if you would like us to share your information with other unaffiliated parties who are not described elsewhere in this policy. Please note that if you consent to the disclosure of your personal information to a third party, that third party may apply its own privacy practices. You should carefully review the privacy notice of any third party before you consent to providing them with your personal information.

In addition, we may share aggregated anonymized information, including non-personal usage data, with third parties for a variety of purposes, including to analyze trends about small business networking and utility use, to show third parties how their products could work with Linksys products and to generally improve small business networking. We've taken steps to ensure that this information cannot be linked back to you and we require third parties to keep all shared information in its anonymized form.

## Where might Linksys transfer my personal data?

Linksys will take all necessary measures to ensure that transfers out of the country where you are located are adequately protected as required by applicable data protection law. The data that we collect from you may be transferred to, and stored at, various locations globally, including the United States, Taiwan, Australia, New Zealand, Canada, the United Kingdom and countries located in the EEA.

If you are located in the EEA, for purposes of the GDPR, transfers of your personal data out of the EEA (if you are a resident of the EEA) will be bound by the EU Standard Contractual Clauses (available [here](#)) pursuant to the GDPR, which the European Commission has assessed as providing an adequate level of protection for personal data, to ensure that your data is protected adequately.

By providing your personal data to us, you fully understand that Linksys may transfer, process and store your personal data outside of your country of residence where data protection standards may be different, and may disclose your personal data to overseas service providers who may not fully comply with the particular laws of your country.

If you are located in Australia, you consent to the collection, use, storage, and processing of your personal data outside of Australia as set out in this Privacy Notice. You consent to the collection, use, storage and processing of your personal data in other countries, without us being responsible under the *Privacy Act 1988 (Cth)* for such use (or for any breach). Where such parties are located outside of Australia, you may have rights to enforce such parties' compliance with applicable data protection laws, but you might not have recourse against those parties under the Australian *Privacy Act 1988 (Cth)* in relation to how those parties treat your personal data.

## How does Linksys aim to keep my personal data secure?

Linksys maintains, and takes reasonable steps to ensure that its service providers maintain, appropriate administrative, technical and physical safeguards designed to protect your personal data against accidental, unauthorized or unlawful destruction, loss, disclosure, and access. Unfortunately, the transmission of information via the Internet is not 100% secure. If you use a computer or device that can be accessed by others, other people may be able to access unencrypted personal data. If you do not want your information to be available to others, exercise caution when using public computers or devices or when using any computer or device to which users unauthorized by you may have access.

We recommend that you take every precaution in protecting your personal data. For example, create strong passwords by using a combination of letters, numbers and symbols, change your passwords often, and make sure you use a secure browser. When creating a password for your SMB network, make sure you choose a unique password that you do not use for other Internet-based services. You should also be aware that names that you give your WiFi-enabled devices may be detectable by Linksys and by others, so you should not include personal data in your device names.

In the event that we are required by law to inform you of a breach to your personal information we may notify you electronically, in writing, or by telephone, if permitted to do so by law.

## **How long will Linksys keep my personal data?**

We will only retain personal data to fulfil the purposes for which it was collected, as required for legitimate business purposes as described in this Privacy Notice, or as otherwise permitted by applicable laws. We may, for example, keep your personal data for a reasonable time after you have stopped using the Service to ensure that Linksys has the records it needs in the event of a dispute or regulatory investigation and to ensure that any ongoing obligations can be complied with, such as complying with requests from regulators. Where personal data is kept, that period will be determined based on the applicable local law.

## **What rights do I have in respect of my personal data?**

You may have a number of rights in relation to your personal data. These can differ by country and jurisdiction.

### ***If you are located in the EEA, you have the following rights:***

**(i) Right of access** – You have the right to confirm with us whether your personal data is processed, and if it is, to request access to that personal data including the categories of personal data processed, the purpose of the processing and the recipients or categories of recipients. We do have to take into account the interests of others though, so this is not an absolute right.

**(ii) Right to rectification** – You have the right to rectify inaccurate or incomplete personal data concerning you.

**(iii) Right to erasure (right to be forgotten)** – You may have the right to ask us to erase personal data concerning you. If required by law we will grant a request to delete information, but you should note that in many situations we must keep your personal information to comply with our legal obligations, resolve disputes, enforce our agreements, or for another one of our business purposes.

**(iv) Right to restriction of processing** – You have the right to request that we restrict processing of your personal data, where you believe such data to be inaccurate; our processing is unlawful; or that we no longer need to process such data for a particular purpose unless we are not able to delete the data due to a legal or other obligation or because you do not wish for us to delete it.

**(v) Right to data portability** – You may have the right to receive personal data concerning you, which you have provided to us, in a structured, commonly used and machine-readable format and you may have the right to transmit that data to another entity.

**(vi) Right to object** – You have the right to object, on grounds relating to your particular situation, at any time to the processing of your personal data, where the justification for our processing is our legitimate interest. We will abide by your request unless we have compelling legitimate grounds for the processing which override your interests and rights, or if we need to continue to process the data to establish, exercise or defend legal claims.

**(vii) Right to withdraw consent** – You have the right to withdraw your consent to our processing of your personal data at any time after you have consented, including opting out of receiving marketing materials. The easiest way to do this is by clicking the "Unsubscribe" link in any email you receive from us.

To exercise any of these rights, please contact us as stated below (**How do I contact you about my privacy rights?**). We will respond to your request promptly upon receipt. For EEA requests, this will be within one month of receipt, or, if further time is required, we will inform you of this and the reason for the delay.

You also have the right to lodge a complaint with the local data protection authority, which may vary depending on your location. Please click [here](#) for a list of contact details for the EEA data protection authorities.

***If you are located in Australia, you have the following rights:***

**(i) Right of access and correction** - You are generally entitled to access personal data that we hold about you. If you request access to your personal data, in ordinary circumstances we will give you full access to your personal data. Depending on the nature of the request, we may charge for providing access to this information, however such charge will not be excessive. However, there may be some legal or administrative reasons to deny access. If we refuse your request to access your personal data, we will provide you with reasons for the refusal where we are required by law to give those reasons.

We take all reasonable steps to ensure that any personal data we collect and use is accurate, complete and up-to-date. To assist us in this, you need to provide true, accurate, current and complete information about yourself as requested, and properly update the information provided to us to keep it true, accurate, current and complete.

Please contact us as stated below (**How do I contact you about my privacy rights?**), if you believe that the personal data is inaccurate, incomplete or out of date, and we will use all reasonable efforts to correct the information. It would assist us to ensure we properly understand your request, and allow us to respond more promptly, if requests are made in writing and include as much detail as possible.

***If you are located in California, you have the following rights:***

**(i) Right of access.** – You may request access to your personal information by contacting us at the address described below. If required by law, upon request, we will grant you reasonable access to the personal information that we have about you. Note that California residents may be entitled to ask us for a notice describing what categories of personal information (if any) we share with third parties or affiliates for direct marketing.

**(ii) Right of deletion** – You may request that we delete your personal information by contacting us at the address described below. If required by law we will grant a request to delete information, but you should note that in many situations we must keep your personal information to comply with our legal obligations, resolve disputes, enforce our agreements, or for another one of our business purposes.

Please address written requests and questions about your rights [here](#) or, if you are in California, call us at 877-460-2323.

We may ask you to verify your identity before we can act on your request. We may conduct an identity verification by phone call or email. Depending on your request, we will ask for information such as your name, the email address connected to your account with us or the date of a support call you made to us. We may also ask you to provide a signed declaration confirming your identity.

In some circumstances, you may designate an authorized agent to submit requests to exercise certain privacy rights on your behalf. We will require verification that you provided the authorized agent permission to make a request on your behalf. You must provide us with a copy of the signed permission you have given to the authorized agent to submit the request on your behalf and verify your own identity directly with us.

If you are an authorized agent submitting a request on behalf of an individual in California, you must attach a copy of the following information to the request:

1. A completed Authorized Agent Designation Form, located [here](#), indicating that you have authorization to act on the consumer's behalf.
2. If you are a business, proof that your business is registered with the Secretary of State to conduct business in California.

If we do not receive both pieces of information, the request will be denied.

## Information for California Residents

California law indicates that organizations should disclose whether certain categories of information are collected, "sold" or transferred for an organization's "business purpose" (as those terms are defined under California law). You can find a list of the categories of information that we collect and share [here](#). If you would like more information concerning the categories of personal information (if any) we share with third parties or affiliates for those parties to use for direct marketing, please submit a written request to us using the information in the "**How do I contact you about my privacy rights?**" section below. We do not discriminate against California residents who exercise any of their rights described in this Privacy Notice.

### How do I contact you about my privacy rights?

Should you have any privacy-related questions or would like to exercise your rights, please contact us [here](#) or, if you are in California, call our toll-free number at 877-460-2323.

If you are in the EEA, for GDPR purposes, our data controller is:

Belkin Limited  
Express Business Park  
Shipton Way  
Rushden, Northants  
NN10 6GL United Kingdom

### Updates to this Privacy Notice

We may update this Privacy Notice from time to time, so please review it frequently. If we change our Privacy Notice, we will post the revised version here, with an updated revision date. If we make material changes to our Privacy Notice, we will notify you by email or prominently post a notice on the Linksys website.

*Last Revised and Updated Effective July 1, 2020*