

# Schlage Base APP Data Privacy Policy

**Release Date:** June 2, 2023

**Effective Date:** June 3, 2023

In this Privacy Policy, we describe the personal data that Allegion Plc. its subsidiaries, and affiliates (collectively “Allegion” “we” or “us”) collects from you, and our use, disclosure, and transfer of that information. This Privacy Policy applies to personal data that we collect from you: (1) online, such as through our applications and Products on which this Policy is posted (collectively, the “Site”); and (2) offline when you interact with us, whether as a customer, vendor, or interested person.

By providing your information to us, you agree that your information, including Personal Data, will be collected, used, and disclosed as described in this Policy. For visitors to our Site, this Policy is incorporated by reference into our Terms of Service.

## Information We Collect

We collect information directly from you, from third parties, and automatically through your use of our Site or any Allegion services. To the extent permitted by law or with your consent, we may combine all of the information that we collect about you from various sources.

**Information We Collect Directly from You.** We collect information from you When you register an account through ‘Schlage Base’ APP, we may collect your contact details, such as your email address, phone number, software password, security questions, and password verification. During your interaction with our Products, we may further collect your nickname, profile picture, country code, language preference or time zone information into your account. When using feedback and suggestion features in our APP, we will collect your email address, mobile phone number and your feedback content to address your problems and solve device failures on a timely basis. When you use this software to set room information, we will collect the room information you set so that you can control the smart devices in each room. When you share the smart device with others in a way permitted and available by this software, we shall collect the sharing account information you provide, the sharing status of the device, your family member information or non-family member information, to enable each user of smart devices to control and use them together.

You are not required to provide us with any personal data, but, you may not be able to take advantage of certain offerings (e.g., registering your lock) if you do not do so.

**Information We Collect About You from Third Parties.** We also may collect information about you from third parties. For example, we may collect your username, name, or e-mail address from social media platforms if you interact with us through social media.

**Information We Collect Automatically.** When you interact with our Product, we automatically collect device information, such as the MAC address of your devices, IP address, wireless connection information, operating system type and version, application version number, push notification identifier, log files, mobile network information and Bluetooth state. During your interaction with our Sites and Services, we automatically collect usage data relating to visits, clicks, downloads, messages sent/received, and other usage of our Sites and Services. When you use our app, the application and exception log may be uploaded. When you connect your Smart Locks with our APP or Services, we may collect basic information about your Smart Locks such as device name, device ID, online status, activation time, firmware version, and upgrade information.

**Sensitive Personal Data.** Sensitive personal data refers to Personal Data that, once leaked or illegally used, may easily lead to the infringement of personal dignity or harm to personal and property safety. We do not collect any type of sensitive Personal Data from you unless otherwise obtain your separate consent in advance.

**Non-personal information.** We may also collect other information that cannot identify specific individuals (that is, information that does not belong to personal information), for example, the statistical class data generated when you use a particular service such as user behavior (including click, page jump, browsing time, search keywords). The purpose of collecting such information is to improve the services we provide to you. The type and amount of information collected depends on how you use our products and/or services. We shall aggregate information to help us provide customers with more useful content about which parts of the software and related services they are most interested in. As far as this privacy policy be concerned, aggregated data is treated as non-personal information. If we combine non-personal information with unidentifiable personal information, such information will be treated as personal information during the combination. **Please understand and agree that we have the right to use the information that has been desensitized and de-identified, and to analyze, process, make statistic the user database and use it for public benefit or commercial purposes without disclosing your personal information.**

## Use of Your Information

We use your information, including your Personal Data, for the following purposes:

- ***To Provide Our Products and Services to You.*** We use your account and profile data, device information, usage data, location information, and Smart Device related information to provide you with our Products and Services that you have requested or purchased.
- ***To Improve Our Services.*** We process your device information, usage data, location information and smart device data to analyze trends and track your use of our site and services as necessary to develop and improve our site and provide our users with more relevant and useful content.
- ***Account management.*** When you register for an account, we shall process your personal data to create and manage the account.

- ***For Vendor Management Purposes.*** We use your information to establish and maintain vendor accounts, provision the requested products and services, and take other actions in furtherance of vendor management. The information that we collect from our vendors is used also for the purposes set forth in this section.
- ***Customer service.*** We use your information for customer service purposes, including for warranty, technical support, or other similar purposes; to respond to your inquiries, and for other purposes for which you contact us.
- ***Communication.*** We use your information to communicate with you, including to respond to requests for assistance. We may communicate with you in a variety of ways, including postal mail, e-mail, telephone, and/or text message.
- ***Administration.*** We use your information for administrative purposes, including to manage our inventory; to help us better understand access to and use of our Site; to provide information and reports to investors, prospective partners, service providers, regulators, and others; to implement and maintain security, anti-piracy, fraud prevention, and other services designed to protect our customers, users, vendors, us, and the general public; to enforce this Policy, our Terms, and other policies.
- ***Research and development.*** We use your information for research and development purposes, including to improve our products, services, and customer experience; to understand our customer and user demographics; and for other research and analytical purposes.
- ***Legal compliance.*** We will process your personal data as we deem necessary or appropriate, including: (a) to comply with applicable laws and regulations; (b) to comply with legal procedures; (c) to respond to requests from public institutions and government authorities; (d) to fulfill our terms and conditions; (e) to protect our operations, businesses and systems; (f) to seek possible remedies or limit damages that we may be required.
- ***To protect us and others.*** We use your information where we believe it is necessary to investigate, prevent or take actions regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person, or violations of our Terms or this Policy.
- ***Marketing.*** We use your information where required by law, to the extent permitted by law, or with your consent (where required by law) for marketing and promotional purposes, including through e-mail. For example, we may use your information, such as an e-mail address, to send news and newsletters, special offers and promotions, or to otherwise contact you about products, services or information we think may interest you. We also may use your information to assist us in advertising our services on third-party websites or through other venues.

It is clarified that any information collected by us is used for the abovementioned purposes only, and the collection, use, disclosure or transfer of such information is necessary for efficient operation and development of Allegion. We do not use, disclose, handle or transfer any information obtained from users for any unlawful purposes.

## **Disclosure of Your Information**

We may disclose your information, including Personal Data, as follows:

- ***Users of Our Site.*** User name and any information that you post to our Site, including without limitation pictures, comments, and text, may be available to all other users of our Site and may be publicly available upon posting.
- ***Affiliates and Subsidiaries.*** We may disclose your information to any current or future affiliates or subsidiaries, for the purposes described above under Use of Personal Data. For example, we may share your information with one of our U.S. entities for storage purposes.
- ***Service Providers.*** We may disclose personal data to third-party vendors, service providers, contractors or agents to enable them to perform functions on our behalf. These service providers may, for example, help us administer our Site, process job applications, or process payments. We may disclose your personal data to customers who access and use our sites and services, and other business partners who, directly or indirectly, provide you with smart devices.
- ***Other Non-Affiliated Third Parties.*** We may disclose your information to non-affiliated third parties, such as wholesalers, distributors, promotional partners and others with whom we have marketing or other relationships for their own marketing purposes. To the extent permitted by law or with your consent, those third parties may use your personal data for their own marketing purposes, such as to market products and services that they believe would be of interest to you.

Specifically, we may disclose your Personal Data to the third parties described in the Addendum.

We also may disclose your information, including personal data, for the following reasons:

- ***Business Transfers.*** We may disclose your information to another entity in connection with, including during negotiations of, an acquisition or merger, sale or transfer of a business unit or assets, bankruptcy proceeding, or as part of any other similar business transfer.
- ***In Response to Legal Process.*** We may disclose your information in order to comply with the law, a judicial proceeding, court order or other legal process, such as in response to a subpoena or other lawful governmental request, including public institutions and government authorities outside your country/territory.
- ***To Protect Us and Others.*** We may disclose your information when we believe it is necessary to investigate, prevent or take action regarding illegal activities, suspected fraud, situations involving potential threats to the safety of any person or violations of our Terms or this Policy, to protect the rights, privacy, security or property of us and/or other users including you, and to seek possible remedies or limit damages that we may be required.
- ***Aggregate and Anonymized Information.*** We may disclose aggregate or anonymized information about you with third parties for marketing, advertising, research or similar purposes.

## Use of cookies and similar technologies

When you use the software, we and service providers on behalf of us may send one or more small data files "Cookies" to your device to identify your browser. Cookies help us measure, for example, the total number of visitors to the software, the number

r of visitors per page, how our users use and interact with the service, and the domain name of the visitor's Internet service provider. You can reset your web browser to reject all Cookies, or send a Cookie in specific time. If you do not want to install Cookies on your device, most browsers allow you to reject Cookies with simple settings. Please note that if Cookies are disabled on your device, certain functions of the software will not work properly.

In addition to Cookies, we may also use similar technologies such as beacons and pixel labels.

## **International Transfers and Offshore Storage of Personal Data**

We may use, disclose, process, transfer or store personal data outside the country in which it was collected. We will transfer your personal data outside of the country in compliance with the legal requirements of the country where you locate, and we will adopt necessary measures as required by the laws in order to ensure your transferred personal data will be sufficiently protected. .

## **Security of Personal Data**

We have taken commensurate steps under relevant data protection laws to protect against unauthorized or unlawful processing of personal data, unauthorized or accidental access to personal data, and accidental or unlawful loss or destruction of personal data. We have adopted technical and organizational measures as specified in the Addendum to protect your personal data. However, we cannot guarantee against any loss, misuse, unauthorized access, unauthorized disclosure, alteration or destruction of personal data or any unlawful forms of processing.

Users should safeguard any password or user ID obtained for use on our Site and are responsible for any misuse or unauthorized use of our Site via their password and user ID maintaining the secrecy of their own passwords. If you have reason to believe that your interaction with us is no longer secure (for example, if you feel that the security of any account you might have with us has been compromised), please immediately notify us using the contact information below.

## **Retention of Personal Data**

We will only retain your Personal Data for the period required to achieve the purposes described in this Policy, unless it is necessary to extend the retention period or is p

ermitted by law. After that, we will destroy it through currently available secure destruction means. If we are unable to destroy the data for technical reasons, we will take appropriate measures to prevent further use of your personal data.

If required to retain Personal Data pursuant to applicable laws, we will retain personal data solely for the retention periods and purposes as required by applicable laws and regulations.

When destroying your Personal Data because it is no longer needed, we will do so in accordance with the following procedures and methods.

- Procedures for destruction
  - We select the Personal Data to be destroyed (e.g., Personal Data whose purpose of processing has been achieved or whose retention period has expired) and destroy it with the approval of our Data Protection Officer.
- Method of destruction
  - If printed on paper, the Personal Data will be destroyed by shredding, incinerating, or some other similar method and, if saved in electronic form, the Personal Data will be destroyed by technical methods (e.g. Low Level Format) which will ensure that the data cannot be restored or recovered.

## Your Rights and Choices

- *Your Rights.* You provide your personal data to us voluntarily. Depending on your jurisdiction, you may have the right, at any time, to access personal data that Allegion holds about you; to request that we stop using or disclosing your personal data; to request that we update, amend, or delete your personal data; and to withdraw any previously given consent with regard to your personal data; using the contact information below. You may make such requests by contacting your country-specific National Data Protection Officer or local Privacy Manager at the Contact Us information provided below.
- *Your Choices.* You can always choose not to provide information, even though it might be needed to take advantage of certain services.
- *Opting Out of Marketing Communications.* We may send your promotional e-mail messages if you request to receive information from us. You may request to stop receiving promotional e-mail messages by following the link contained in the e-mail itself. Please note that if you opt out of receiving e-mail marketing communications from us, we may continue to communicate with you for other purposes (e.g., to respond to your inquiries or for service-related purposes). You may otherwise opt out of receiving marketing communications from us by contacting us at the mailing addresses set forth in the Contact Us section below.

## Children's privacy

Protecting children's privacy is very important to us. This software is not available for individuals under the age of 14, and we request that these individuals do not provide us with any personal information. We do not intentionally collect personal information about children under the age of 14, unless we have the consent of a parent or legal guardian. If we collect the personal information of children under 14 without the consent of their parents or legal guardians, we will delete the information when we learn of this situation.

## The scope and effectiveness of this policy

This policy applies to your use of the software services.

The service may include other websites, online service links, other services or functions operated and maintained by third parties that are not controlled or maintained by us, or services provided to you by third parties based on the software. The information you provide to such third parties will be subject to the privacy policy of such third parties and will not be subject to this privacy policy. **We are not responsible for how third parties use the personal information they collect from you, nor can we control its use. When you use these products or services, we recommend you to read carefully the privacy policies of such third parties in detail and determine whether to agree to the privacy policies and whether to continue using the products or services.**

This privacy policy is an important part of the software license and service agreement. If there is any inconsistency between the privacy policy and the software license and service agreement, the privacy policy shall prevail; If not mentioned in this privacy policy, the software license and service agreement shall prevail.

The headings of all terms of this policy are for ease of reading only and cannot be used as the basis for interpreting the meaning of this policy.

This privacy policy exists in both English and Chinese versions. In case of any conflict between the English version and the Chinese version, the Chinese version shall prevail.

## Changes to this Policy

We may change this Policy from time to time, so please be sure to check back periodically. We will post any changes to this Policy on our Site. If we make any changes to this Policy that materially affect our practices with regard to the Personal Data we have previously collected about you, we will endeavor to provide you with notice in advance of such change by highlighting the change on our Site or e-mailing you. Your continued use of our Site, purchase of our goods or services or provision of further information constitutes your acceptance of our revised Policy.

## Contact Us

Please contact us at **4009201818** or give your feedback through APP if you have any questions or concerns about this Policy, the Personal Data we have about you, require assistance in managing your choices, or have other questions, comments or complaints regarding our privacy practices.

Allegion Security Technologies (China) Co., Ltd.

## Addendum

### 1. Transfer of personal data to third parties

Specifically, Allegion provides personal data to or outsource the processing thereof to third parties as specified below.

#### (a) Provision of personal data to third parties

Name of recipient	Purposes of use and collection by recipient	Items of personal data accessed by or disclosed to the recipient	URL
Tuya Inc	Provide software service for both user management and device management.	User account information, name, email address and/or phone number, mailing address, username and login credentials. Mobile Device Access Information: When you interact with our website and services through hardware, we automatically collect device information, such as the device's unique device identification identifier, serial number, Internet Protocol Address, wireless connection information, operating system type and version, Browser type and version, push notification identifiers, and mobile network information. Lock Device Information: When you connect your lock device to the app, we automatically collect device information, such as the device's unique device identification identifier, serial number, Internet Protocol Address, lock serial number, lock battery, lock open and close event records, door status.	Privacy Policy Address: <a href="https://auth.tuya.com/policies/privacy">https://auth.tuya.com/policies/privacy</a>
Shenzhen Tencent Computer System Co., Ltd	Provide infrastructure, including network, server and virtualization services	Website hosting, data analytics, infrastructure provision, IT services, customer support services, email delivery services and other similar services, all information will be stored on Tencent Cloud, please refer to the Privacy Policy for details	Data processing and security protocols: <a href="https://intl.cloud.tencent.com/zh/document/product/301/17347">https://intl.cloud.tencent.com/zh/document/product/301/17347</a> Privacy Policy Address: <a href="https://intl.cloud.tencent.com/zh/document/product/301/17345">https://intl.cloud.tencent.com/zh/document/product/301/17345</a>
Xiaomi Mobile Software Co., Ltd.,	Push notification function	information collection details: your OAID (applicable to Android Q and above), MEIDMD5, Android ID, VAID, AAID, as well as your MID (applicable to MIUI system), device model information.	Privacy Policy Address: <a href="https://dev.mi.com/console/doc/detail?pId=1822">https://dev.mi.com/console/doc/detail?pId=1822</a>
Huawei End Point Co., Ltd	a) provides push notification services; b) counts the success rate of Huawei push SDK interface calls	information collection details: basic application information, in-app device identifier, device hardware information, system basic information and system settings information	Privacy Policy Address: <a href="https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050042177">https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050042177</a>
Guangzhou Huantai Technology Co.Ltd	Push notification function	information collection details: your device-related information (Serial Number, User ID, Android ID, Google Advertising ID, mobile phone Region settings, device model, mobile phone battery, mobile operating system version and language), application information using the push service (APP package name and version number, running	Privacy Policy Address: <a href="https://open.oppomobile.com/wiki/doc#id=10288">https://open.oppomobile.com/wiki/doc#id=10288</a>

		status), push SDK version number, network-related information (IP or domain name connection result, current network type), message sending result, notification bar status (notification bar permissions, user click behavior), lock screen status (whether the screen is locked, whether the screen is allowed to be locked)	
Vivo Mobile Communications Co., Ltd.	Push notification function	information collection details: device and application information: including operating system version number, application information, device identifier (SIM, mobile country code and vivo Android device) during your use of vivo devices and services Mobile network number), mobile operator, language used, system settings, device and application data	Privacy Policy address: <a href="https://www.vivo.com.cn/about-vivo/privacy-policy">https://www.vivo.com.cn/about-vivo/privacy-policy</a>
Autonavi Software Ltd (Autonavi SDK)	Provide corresponding services, provide you with problem tracking, troubleshooting, diagnostic services and conduct data statistics to ensure the normal operation of products and services, Autonavi will process your device information, including IDFA, Android ID, MEID, MAC address, OAID, sensor, hardware serial number, based on different devices and systems (Android/iOS) and system versions. In particular, when you use the following Autonavi SDK-related functions and services, the device information collected will be different. For details, please check the content of the Location SDK, Map SDK, Search SDK and Navigation SDK	<p>Locate SDK details collection:</p> <p>Location information: The purpose of use is to return the user's location information to the application, and for developers to provide corresponding services based on the user's location information; in order to facilitate the provision of real-time road conditions and road condition prediction services, we will conduct data statistics and analysis on the user's location information, and make judgments on traffic congestion conditions based on this</p> <ul style="list-style-type: none"> <li>• Mobile device information: The purpose of use is to provide services, track, troubleshoot, diagnose, and count various problems in the service, and ensure the normal operation of products and services</li> </ul> <p>Map SDK details collection:</p> <ul style="list-style-type: none"> <li>• Location information: The purpose of use is that when the developer turns on the positioning small blue dot function, in order to return the user's location information to the application, display the user's location on the map and provide the developer with corresponding services based on the user's location information</li> <li>• Collect equipment information: The purpose of use is to provide services, track, troubleshoot, diagnose, and count various problems in the service, and ensure the normal operation of products and services</li> </ul> <p>Search SDK details collection:</p> <p>Mobile device information: The purpose of use is to provide services, track, troubleshoot, diagnose, and count various problems in the service, and ensure the normal operation of products and services</p>	Privacy Policy Address: <a href="https://lbs.amap.com/pages/privacy/">https://lbs.amap.com/pages/privacy/</a>

**(b) Outsourcing of the processing of personal data to third parties**

Outsourced processors	Outsourced tasks
Tuya Inc	User register, Login, Delete and other user related tasks.

**(c) Cross-border outsourcing of the processing/storage of personal data to third parties**

Recipient (if the recipient is a corporation then the name of the corporation and the contact information of the person in charge of the management of personal data)	Items of the personal data to be transferred	Countries where the personal data are to be transferred and the date, time, methods of transfer	Purposes of use of recipient	Periods of retention of recipient
None	None	None	None	None

**(d) Data Center for Country or Region in user data storage:**

For user in the following country or regions, the user/device data will be processed and stored in each data center. Within the lifecycle of the data for user and devices, there will be no cross data center outsourcing processing and storage.

Country	Data Server location
South Korea	Western America Data Center
Thailand	
Vietnam	
Malaysia	
Indonesia	
Philippines	
Singapore	Central Europe Data Center
China	China Data Center
India	India Data Center

**2. Security**

We will implement technical, organizational, and physical security measures prescribed by applicable laws in order to protect data, such as those listed below:

- Managerial measures: Designation of a data privacy officer, establishment and implementation of an internal management plan, regular training of employees on data protection, etc.;
- Technical measures: Management of access authority to the personal data processing system, installation of an access control system, installation of security programs, etc.; and
- Physical measures: Restriction of access to personal data storage facilities and equipment such as computer rooms and data storage rooms, etc.