Washington State Residents: Click HERE for the Washington State Consumer Health Privacy Policy

---

US Residents:

Home Connect App Privacy Policy
United States

BSH Home Appliances Corporation, 1901 Main Street, Suite 600, Irvine, CA 92614 ("Home Connect" or "we") is responsible for the collection, processing, and use of your Personal Information associated with the Home Connect App (the "App"). We collect, process, and use Personal Information that is entered by you or otherwise created and processed during your use of the App, the associated household appliances, or services offered by Home Connect in accordance with applicable data privacy laws. This Privacy Policy explains how we treat such data.

This Privacy Policy applies exclusively to the App and does not apply to any product or service other than the App.

1. Types of Personal Information collected from you and your device

Home Connect collects, processes, and uses your Personal Information in connection with your use of the App, the associated household appliance and services, and functions offered by Home Connect (“Services”).

“Personal Information” means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, to an individual.

a. User master data and usage data

We may collect and use your Personal Information when you set up a user account (register) and when you set up the App. This data is stored in your account. Your account is personal and non-transferable.

When you register with a SingleKey ID, we may collect and store access data, i.e. identification data that controls access to a SingleKey ID user account and consists of the user ID (user email address and phone number). Bosch.IO GmbH, Ullsteinstrasse 128, 12109 Berlin, Germany ("BIO") is responsible for providing this registration service.

During the registration process, including when setting up of the App or registering for a central BSH user account (if not transmitted via a SingleKey ID), we may collect additional Personal Information from you, including:

- First and last name
- Email address (also used as your user ID)
- Country in which you operate your household appliance
- Password as access protection for the App/central BSH user account

Information collected during the registration process may differ by country. The information is managed (if available) via a central BSH user account, which can also be used as a Home Connect account. Information we collect and store during the registration process and while using the App may include:

- Language setting of your mobile device
- System settings related to the App (e.g. permission to send in-app messages)
- Consent to and recognition of the Terms of Use
- Acknowledgement of this Privacy Policy
- Marketing consents and their scope where legally required
- User account status (activated/deactivated)
- Default App tracking settings (varies by country, see Item 7 for more information)
- Service history of connected household appliances

- Order history (e.g. consumables)

- Detergent Scan: if this service is available for your appliance and you use it, we store the water hardness and detergent used in the App. A "detergent history" is created in the App. You can delete this history at any time.

- Approximate device location derived from the zip code or shortened IP address (e.g. at the municipality level) to improve user experience, for example, by helping to set location-based device settings such as water hardness in your region or local time zone

- Content you upload to the App, such as recipes, recipe images, labels, including the information required for you to share content with third parties (e.g. your name as the creator of the recipe). To share your own recipes with others, you must create a separate cooking profile for that purpose and choose a name and avatar for the profile, which will be displayed with your shared recipe. The name and avatar do not have to relate to you as a person and can be an alias.

b. Appliance master data

We collect and use the following data concerning the connection between your household appliance and user account:

- Brand of the household appliance

- Serial number and, if applicable, manufacture date of the appliance (E number (full model) and FD (production) number can also be found on the appliance label)

- Unique identifier of the network adapter installed in the household appliance (MAC address)

- Additional programs you have purchased for your appliance via the App. Additional programs are linked to the appliance, not your user account, and remain in the appliance (but not in your user account) if you sell or otherwise transfer the appliance. Additional programs are generally not transferable to other home appliances.

This data is allocated to your user account for each connected household appliance under the "Home Connect" function.

c. Appliance usage data

We collect and use the following data related to the usage of the appliance:

- Selected basic settings, program selection, and preferred program settings on the appliance or via the App

- Appliance status data such as ambient conditions, condition of parts, changes of appliance status (e.g. mode of operation, open or closed doors/front panel, temperature changes, fill levels), appliance status messages (e.g. appliance is overheated, water tank is empty), and error messages (including error reports)

- Individual appliance settings/contents including free-text fields (e.g. digital map for vacuum cleaner robots, beverage name for coffee machines, downloaded or self-designed recipes)

- Video and/or image data (e.g. vacuum cleaner robots, stoves, ovens, and refrigerators with built-in cameras) used for functions of the appliance, including, but is not limited to, imaging the contents of the refrigerator and, in some cases, the area visible to such cameras when the refrigerator door is open (Camera in the Fridge) as well as image data detecting the degree of browning (Camera in the Oven).

If you allow another user (via their own account or via your account) to use home appliances via the App, the appliance usage data created by the additional user will also be stored.

d. App related usage data and app download origin data

App related usage data are generated by your interaction with the App, such as the features you use, click behaviour for App controls, drop-down menu selections, on/off switch settings, information from A/B and multi-variant tests (i.e. tests of how different versions of our App are accepted by the user), error reports, and interactions of your App with third-party applications, such as web pages that you open from within the App. See item 7 for more information.

The App may use the tracking technology “Adjust” provided by Adjust GmbH, Saarbrücker Str. 37A, 10405 Berlin, Germany ("Adjust"). You can find information about Adjust and its privacy policy at https://www.adjust.com/privacy-

policy/. When you follow links on our websites and then launch the Home Connect App after downloading it from an app-store, Adjust processes install event data (such as the website you started the download from). This helps us understand how our users are interacting with links to optimize and analyse our app attribution model. For that analysis, Adjust uses your mobile identifier (e.g. IDFA or Google Play Services ID), and your pseudonymized (hashed) IP- and possibly MAC address. Adjust also tracks usage frequency of the Home Connect App. The information gathered may identify you directly or indirectly as an individual user of the App, as the information collected is typically linked to a pseudonymous identifier associated with the device you use to access the App. We use the information to understand how our products are used, improve or develop new features or functionality for our products, notify you of your product usage and performance, and market products and services to you. We may use and disclose information on an aggregate for research and marketing purposes. You can choose at the start of the Home Connect App whether you allow tracking by Adjust. If you choose not to be tracked, even if you use a link on our Websites, you will not be tracked.

2. How we use collected data

We use the data described in item 1 for the following purposes:

- To provide App features, services via the App, and updates for your device (1.a. to c.)
- For notification purposes, including promotional push notifications or alerts sent to your device (1.a. to c.)
- For maintenance purposes, including in-app/email messages providing recommendations on the use of settings and/or maintenance programs, identifying anomalies that indicate a potential major malfunction of the appliance which may be avoided by taking appropriate measures (e.g. if vibrations in the appliance indicate an imbalance that could damage the appliance), and offering reactive troubleshooting (e.g. in the context of remote diagnosis, during on-site repair, or at the repair center) of connected household appliances (1.a. to c.)
- To improve the App (including interaction of the App and appliance) and to troubleshoot the App and digital services offered through the App (1.c. and d.)
- To improve a range of products and services offered by BSH and affiliated companies, especially with regard to home appliance usage (e.g. programs which are not used and/or which are frequently used) and features of the App and appliance, including algorithmic learning (e.g. to improve the detection of the level of contents stored in refrigerators or the degree of browning in the oven) (1.c. and d.)
- For billing purposes, insofar as appliances connected to the App or the services offered in the App provide for usage-based billing (1.a. to c.)
- For marketing and market research purposes including in-app/email messages (1.a. to c.)
- To understand how our products are used, improve or develop features or functionality for our products, notify you of your product usage and performance, and market products and services to you. We may use and disclose information on an aggregate basis for research and marketing purposes.
- Name, contact details and appliance master data (including customer service transaction data) are kept in a separate "Safety Action" database to perform product recalls
- In anonymized form for statistics on the use of connected appliances for use by Home Connect and its affiliates for internal purposes and in the context of general communications, including social media (1.c anonymized)

Regarding other data transfers within the Bosch Group associated with a central SingleKey ID, refer to the BIO data protection information at https://singlekey-id.com/en/data-protection-notice/.

3. General retention periods

Absent statutory provisions to the contrary, the following retention periods apply:

- ***SingleKey ID:*** Deleted upon deletion of the SingleKey ID user account.
- ***User master data:*** Deleted upon deletion of the local user account or central BSH account.
- ***Appliance master data:*** Link to the user account removed upon removing the appliance from the user account.

- ***Appliance usage data:*** User-specific storage for thirty (30) days, after which data is stored in pseudonymized form and in personalized form for services and/or repair services provided via the App or on-site (including maintenance/troubleshooting) for the duration of the contract or while the function is activated (if the function can be disabled). If you have shared content with third parties, that content is not deleted and may remain on the appliance and/or end device of the third parties with whom you have shared the content.

- ***App related usage data and app download origin data:*** Storage in pseudonymised form and provision in personalized form for services/messages provided via the App to the extent that the "Enable usage-data tracking" function is activated. Deactivating the function resets the individual ID used for tracking, so that App usage data already collected can no longer be connected to you.

- ***Name, contact details and device master data (including customer service transaction data):*** Stored in personal form for 30 years in a separate "Safety Action" database held solely to conduct product recalls.

If you sell the home appliance, you must reset the appliance to its factory settings before deleting the SingleKey ID or the App. If you have allowed the use of an appliance together with another app user who does not use their own account, deletion of your account triggers the deletion of the other user. If you have allowed the use of a home device together with another app user who uses their own account, deletion of your account does not trigger the deletion of the additional user. If you do not want the other user to be able to continue using the appliance via the App, you must arrange for the deletion of the other user. If such deletion does not take place, the previously collected appliance master data and appliance usage data will remain available for the additional user.

4. Data processing management

a. Connectivity of your household appliance

You can use the App to manage the connectivity of your household appliance.

If required and if your appliance provides for this function, you can set up the connection to the Home Connect server such that each appliance is connected separately (*Appliances → Settings*). After doing this:

- appliance usage data (1.c.) will no longer be transmitted to the Home Connect server; if your appliance is equipped with buffer memory, the appliance usage data will be transmitted to the Home Connect Server in the event that the Wi-Fi connection of your appliance to the Home Connect Server is restored.

- certain App features will no longer be available; the App cannot be used to operate the appliance, even if an internet data link is set up.

You can switch off the Wi-Fi connection for an individual appliance (*Appliances → Settings*), after which:

- appliance usage data (1.c.) will no longer be transmitted to the Home Connect server; if your appliance is equipped with a buffer memory, the appliance usage data will be transmitted to the Home Connect Server in the event that the Wi-Fi connection of your appliance is restored.

- the appliance may only be operated from the appliance itself, not via the App.

b. User accounts and local App data

You can manage your user accounts via the App and delete locally stored App data.

You can delete your user account ("*Profile*" → "*Personal Information*" → "*Delete account*"), after which:

- the connection between your appliance and your user account will be deleted.

- your appliance will no longer send appliance usage data to the Home Connect server provided no other user accounts are linked to the appliance (see item 1.a.).

By deleting the App or using the “Full reset” function, all locally stored user-related data will be removed, but not the accounts which were created separately. Some App features do not store user-related data locally. You can have such data deleted by contacting the Home Connect Service Hotline at 1-800-944-2904.

To delete the central BSH user account, use the function provided in the account.

If you use the SingleKey ID, the SingleKey ID account will be deleted via the SingleKey ID functions, whereby in addition to the SingleKey ID itself, individual linked applications can also be deleted. If the SingleKey ID is the only access mechanism to the App/to the central BSH user account, deleting the SingleKey ID may make access to the linked services impossible. Before deleting the SingleKey ID, please check if you still have linked applications/user accounts.

Content you uploaded to the App (e.g. recipes, recipe images) and shared with third parties will remain on the third party's appliance even if you delete the data locally.

c. The household appliance's factory settings

You can reset your household appliance to its factory settings. After doing this:

- the appliance will lose its connection to the Home Connect server due to the network settings being reset.
- the appliance will no longer be linked to any previously associated user account (which requires the appliance to be connected to the Internet) and it will not be displayed in the App.
- all contents stored on the appliance will be deleted.

Please read your appliance's user manual before restoring the factory settings.

5. Transmission or disclosure of your data

a. Information Disclosed to With Our Service Providers

We work with service providers to create and run the App and provide related services. To the extent that we have bound these service providers to process data in line with strict instructions in their capacity as data processors on our behalf, any data processing activities undertaken by such providers shall not require your consent. The service providers we have commissioned to create and run the App include service providers for hosting services, programming services, hotline services (also performed via a chat function or similar communication channels), as well as other App services.

We transmit your data to service providers whose offers and services can be used in connection with the App or where the App enables access to such services (see item 10). We also transmit your data to other recipients where necessary to fulfil a contract with you or between you and the third party, where we or the recipient has a legitimate interest in the disclosure of your data, or where you have given your consent to that transmission. These recipients include service providers and affiliate companies within our corporate group.

The chat feature available in the App enables you to communicate with an AI chatbot powered by the Microsoft Azure AI platform. Your interaction via the chat feature may be collected, recorded, and stored for customer service and quality control purposes. By using the chat feature, you consent to the collection, processing, and use of your Personal Information. At the outset of your interaction with the chat feature, we will present you with and obtain your consent to the terms of this Privacy Policy.

Content you have created, such as recipes, may be transmitted to other BSH companies (domestically and internationally) within the scope of technical processing and provision of the content/services. We base such transmission/processing on data protection agreements between the BSH companies involved.

b. Information Disclosed in Connection with Business Transactions

We may disclose your Personal Information to a third party in the event of reorganization, merger, sale, joint venture, assignment, transfer, or other disposition of all or any of our business, assets, or stock, including in bankruptcy or a similar proceeding.

c. Information Disclosed for Our Protection and the Protection of Others

We may disclose your Personal Information if we are obligated to do so due to legal provisions, enforceable administrative or court orders, or pursuant to a request from a governmental entity, or if we believe in good faith—after considering your privacy interests and other factors—that such action is necessary to:

- Meet legal requirements or comply with legal processes (e.g. subpoenas)
- Enforce our terms of use and contracts, including for billing and collections

- Protect our rights and safety (including property rights) or the rights and safety of a third party, our affiliated companies, or the public

- Stop activity that we consider illegal, unethical, or legally actionable

d. Information Disclosed in an Aggregated or Anonymized Manner

We may share information about our App with our business partners, affiliates, and other third parties so that they can understand you and how you use our App for the purpose of advertising on our sites or the sites of other parties with which we have a business relationship. This information is not considered Personal Information because it is anonymized and aggregated in such a way that it cannot reasonably be linked to you.

e. Information Disclosed to Others in Accordance with Your Preferences

We may disclose Personal Information to third parties if you consent to such disclosure. When configuring your profile, you may indicate that you would like to receive information about opportunities, products, or services of third parties.

You have the option to connect your appliance (via your Home Connect account) with compatible third-party services, such as Amazon Alexa, Fit Bit, Side Chef, and others. If you connect your appliance to such third-party services, we will disclose your data to the relevant third party for the purpose of carrying out the requested services. Your use of third-party services is governed by the third party's terms of use and privacy policy. We encourage you to review the terms of use and privacy policies of relevant third parties for information about their practices.

6. Location of processing and information

Personal Information collected in accordance with this Privacy Policy may be transferred to, processed in, and stored in the United States and all member states of the European Union. Privacy laws in other jurisdictions may differ from U.S. privacy laws and your Personal Information may be accessible to governmental authorities, law enforcement, or the courts in such jurisdictions.

Should you relocate your appliance outside the U.S. or use the App outside of the U.S., you may be subject to different terms of use and a different privacy policy or data protection statement.

7. Recording App related usage data

The App may record data on App related usage (see item 1.d.). Depending on your country of residence and operating system, your consent is obtained accordingly or you have the option to change consent once it has been activated, as described below. The following analytics services and service providers are used for recording App related usage data:

- Adobe Systems Software Ireland Limited, 4-6 Riverwalk, Citywest Business Campus, Dublin 24, Ireland.

- Adjust Tools by Adjust GmbH, Saarbrücker Str. 37a, 10405 Berlin, Germany.

- Optimizely Inc., 631 Howard Street, Suite 100, San Francisco, CA 94105, United States.

If the "Enable usage-data tracking" function is activated, App related usage data will be sent to and stored on servers of providers located in the European Union. The App related usage data enables us to analyse how you use the App and provide messages (in App or email) to you for services provided via the App (see item 1.d.). IP anonymisation is activated for this App, which means that the IP address you use is truncated before being sent to the server. The analytics providers will use this information on behalf of Home Connect to evaluate how you use the App, generate error reports, and to prepare reports on App activity for Home Connect.

A/B and multi-variant tests are performed on our behalf by Optimizely. For this purpose, app-related usage data is collected, transmitted to an Optimizely server, and stored and processed there. Such analysis enables us to improve the App, to better understand and improve app usage and the connection of home devices, and to provide contextual content in the App and on websites you use. To provide contextual content, we build typical usage profiles (so-called "audiences") that enable us to provide content in a way that is appropriate for you. IP addresses transmitted from your mobile device and other Personal Information within the context of these analytics activities will not be merged with other data held by analytics providers or Home Connect without your consent.

You can control whether App related usage data is recorded and processed in the personal settings within the App or in the corresponding system menu of your mobile device. Depending on the laws in your country, the analytics and/or tracking function may be activated by default, but you may change these settings at any time.

In addition, error reports from the App can be sent to us so that we can eliminate errors. These reports are used on a personalized basis to analyse and correct the error in the event of a specific error report from you. Without direct personal reference, error reports are used to eliminate errors for all App users and to avoid future errors as far as possible.

If covered by a separately declared consent (e.g. a marketing consent given by you via the website), we may also use the app-related usage data within the scope of this consent to personalize the corresponding (marketing) communication to you and your interests. In the context of such consent, we inform you about such possible use.

8. Error reports

We use tools (e.g. Visual Studio App Center (https://appcenter.ms)) to collect and send anonymous error reports if the App crashes or performs in an unintended or unexpected way. Our service providers and Home Connect receive error reports only with your consent. We will request your consent each time we wish to transmit such information.

9. Data security

We deploy reasonable technical and organizational measures to protect your data from manipulation, loss, and unauthorised third-party access. These measures include the use of encoding technologies, certificates, firewalls on the Home Connect servers and password protection in the Home Connect App. The data security level of the Home Connect App has been tested and certified by TÜV Trust IT. We are continually reviewing and improving our security measures in accordance with technological advancement. However, no method of transmitting data over the internet is 100% secure and we therefore cannot guarantee the absolute security of the Personal Information that we maintain.

If your mobile device is sold or passed on to a third party, be sure to first log out of your account and delete the App. It will then no longer be possible to (re)assign the mobile device to your user ID or Appliance. If you sell the Appliance, be sure to restore the factory settings. This will sever the link between the appliance and your account.

If you purchase a previously owned appliance, check the account settings in the App to make sure that no unknown users are linked to the appliance. In case of doubt, restore the factory settings to protect your Personal Information.

10. Scope of application of the data protection information

This data protection information shall apply for the functions and services offered by Home Connect via the App. For additional functions or services offered within the App by Home Connect or a BSH Group company, special information on data protection is provided, insofar as their use is subject to special data protection regulations or information.

This data protection information does not apply for third-party services, even if Home Connect facilitates the use of and/or access to such third-party services in the App (such as video files available in the App). The use of third-party services is governed by the data protection provisions of the third-party service provider and, if applicable, additional data protection information on our part which outline the distinctive features of these third-party services and shall only be relevant in this regard. As your use of third-party services is governed by such third party's privacy policy, whose practices may differ from Home Connect, we encourage you to review the third party's privacy policies for information about their practices.

If you are referred to another service provider, Home Connect will make reasonable efforts to elucidate that referral (e.g. by embedding the service provider's content within the App using inline frames) if such referral is not clear. If you click on a link in the App which calls up an app or website of another service provider, this is considered a clear referral.

11. Multiple users

The Home Connect App may be used by multiple users, as set out in the Terms of Use. The data sent to third-party service providers may contain appliance usage data pertaining to the usage behaviour of other appliance users.

12. Children

The Home Connect App is for use by persons that are at least 18 years old. We do not knowingly collect Personal Information from a person under 18. If we discover or are notified that we have collected Personal Information from a person under 18, we will delete that information from our systems.

13. Changes to the Privacy Policy

Home Connect reserves the right to revise or supplement this Privacy Policy by publishing a new version here. Home Connect will provide the most update-to-date Privacy Policy in the App. Please review the Privacy Policy periodically. By continuing to use the App, you are deemed to consent to current Privacy Policy, including revisions or supplements.

14. Rights and withdrawing consent

You may request that we correct inaccuracies in your Personal Information. You also may withdraw your consent for us to collect, process, and use your Personal Information at any time with effect for the future. Generally, consent may be withdrawn using the respective App setting or through the contact information provided in the App. Withdrawing your consent may result in reduced functionality of the App and/or prevent you from using the App altogether. For technical or organizational reasons, there may be an overlap between you withdrawing your consent and your data being used. Data required for billing and accountancy purposes, or which are subject to the legal duty to preserve records, are not affected by this.

15. Notice to California Residents

The California Consumer Privacy Act and California Privacy Rights Act (collectively "CPRA") provide residents certain rights regarding the Personal Information that businesses collect and how the collected personal information is used.

a. Notice of Information We Collect

Pursuant to CPRA, this serves as notice of the categories of Personal Information that we collect through the App and the specific business or commercial purposes for which the Personal Information was collected. Please see Section 2 for the specific commercial purposes for which Personal Information was collected, and Section 3 for the general retention periods of such collected Personal Information.

We collect Personal Information about you from you, including through your use of our App and our services, from our affiliate companies, and from third parties. In particular, the App has collected the following categories of Personal Information from California consumers within the last twelve (12) months:

- Contact Information (e.g. name, email address)
- Device Information: type of device on which the App is used or downloaded, operating system name and version of the device used to access the App, device manufacturer, App version accessed on your device, device ID, IP address, and geolocation data
- App Usage Data: information related to your in-app preferences such as preferred language, purchase history, device history, and maintenance history
- Demographic Information (e.g., zip code, age, preferences, gender, race or ethnicity, interests, favorites)

b. Personal Information Disclosed for a Business Purpose

In the past 12 months, we have disclosed the following categories of Personal Information for a business purpose to the third parties listed below:

Category of Personal Information	**Third Parties to Whom Personal Information is Disclosed**
Contact Information	Affiliates, service providers, business partners, parties to a corporate transaction or proceeding, public authorities or in legal proceeding
Device Information	Affiliates, service providers, business partners, parties to a corporate transaction or proceeding, public authorities or in legal proceeding
App Usage Data	Affiliates, service providers, business partners, parties to a corporate transaction or proceeding, public authorities or in legal proceeding
Demographic Information	Affiliates, service providers, business partners, parties to a corporate transaction or proceeding, public authorities or in legal proceeding

c. Your CPRA Rights

- **Right to know or confirm what Personal Information is collected**. You may request that we disclose to you the following information:

  - categories of Personal Information BSH has collected about you
  - categories of sources from which Personal Information was collected
  - purpose for which your Personal Information was collected
  - categories of third parties to whom BSH discloses Personal Information
  - specific pieces of Personal Information BSH has collected about you

- **Right to request deletion of your Personal Information**. You may request that we delete any Personal Information that we have collected from you, provided that we may retain Personal Information as authorized under the CPRA, including, but not limited to, retaining Personal Information necessary to provide our services, detect security incidents, protect against malicious, deceptive, fraudulent, or illegal activity, debug to identify and repair errors on the App, enable solely internal uses that are reasonably aligned with your expectations based on your relationship with us, comply with a legal obligation or otherwise use your Personal Information, internally, in a lawful manner that is compatible with the context in which you provided it.

- **Right to correct inaccurate Personal Information**. You may request that we correct inaccuracies in your Personal Information. When you submit a request to correct inaccurate Personal Information, you will need to specifically identify the information that is incorrect and provide the correct information.

- **Right of no retaliation following exercise of CPRA rights**. We will not discriminate against you if you exercise one or more of your CPRA rights.

We do not sell or share your Personal Information as that term is defined in CPRA or under Nevada Law (Section Chapter 603A of the Nevada Revised Statutes). Given that we neither "sell" nor "share" Personal Information for CPRA purposes, we do not provide a mechanism to opt out of such disclosures pursuant to CPRA.

To the extent we collect any Sensitive Personal Information (as defined under CPRA), we do not use your Sensitive Personal Information for purposes other than those set forth in Modified Proposed CPRA Regulations § 7027.

d. Exercising Your CPRA Rights

If you are a California resident who has provided Personal Information to BSH or who reasonably believes that BSH collected or stores your Personal Information, you may exercise your rights under the CPRA by one of the following methods:

- submitting a request online at https://datarequest.bsh-group.us/en/form?c=us
- emailing a request to bsh-us-dataprotection@bshg.com
- calling our toll-free number (855) 769-1755

If you email or call, please include your name, address, and phone number or email in all communications and state clearly the nature of your request.

To process your request to know, delete, or correct your Personal Information, we will need to verify your identity using commercially reasonable means. If you have a password-protected account with us, we may verify your identity through our existing authentication practices for your account. If you do not have an account with us, we may request from you two or more data points of personal information to verify your identity to the extent legally permitted.

We cannot respond to your request or provide you with personal information if we cannot verify your identity and authority to make a request. If you are a member of a household making a request, you represent that you have the right to request information relating to the household. We may also individually verify all members of the household before responding to a request.

e. Authorized Agent

As a California resident, you have the right to designate an agent to exercise these rights on your behalf. When you submit a request to know, delete, or correct your Personal Information through an authorized agent, we may require

that you (i) provide us a copy of your written permission for the authorized agent to submit the applicable request, and (ii) verify your own identity directly with us.

Please use this form or contact us at bsh-us-dataprotection@bshg.com for more information if you wish to submit a request through an authorized agent.

f. Response Timing and Format

Once you submit a verified request, we will send you a receipt acknowledging your request within 10 days. If you do not receive a receipt within 10 days of submitting request, please email bsh-us-dataprotection@bshg.com, as an error receiving your request may have occurred. We endeavor to respond to verified requests within 45 days after receipt. If we require more time, this process may be extended an additional 45 days (90 days total), as permitted under the CPRA. We will inform you of the extension period in writing.

Our response to your request will be sent from bsh-us-dataprotection@bshg.com. Our response, including any Personal Information, may be sent as an encrypted file.

16. Special Notice to Colorado, Connecticut, Delaware, Florida, Iowa, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Tennessee, Texas, Utah, and Virginia Residents

This section describes the Personal Information (including "Personal Data" as defined by applicable statute) we collect or process about residents of the states identified above and your rights pursuant to the Colorado Privacy Act, Connecticut Data Privacy Act, Delaware Personal Data Privacy Act, Florida Digital Bill of Rights, Iowa Consumer Data Protection Act, Maryland Online Data Privacy Act, Minnesota Consumer Data Privacy Act, Montana Consumer Data Privacy Act, Nebraska Data Privacy Act, New Hampshire law with respect to the expectation of privacy, New Jersey concerning online services, consumers, and personal data, Oregon Bill Relating to Protections for the Personal Data of Consumers, Tennessee Information Protection Act, Texas Data Privacy and Security Act, Utah Consumer Privacy Act, and Virginia Consumer Data Protection Act.

a. Your Rights

Under the laws of the states listed below, consumers who are residents of these state may have specific rights regarding their Personal Information. When required and permitted, we will respond to most requests within 45 days unless it is reasonably necessary to extend the response time. Subject to certain limitations, you may have the following rights depending on your state of residence. Please note that these rights do not extend to an individual acting in an employment context.

i. Colorado, Connecticut, Montana, Nebraska, New Hampshire, New Jersey, Tennessee, Texas, Virginia

- **Right of Access**: The right to confirm whether we process your Personal Information and request to access to such Personal Information.
- **Right to Deletion**: The right to request that we delete Personal Information we have collected about you.
- **Right to Data Portability**: The right to request that we provide you with your Personal Information in a portable format.
- **Right to Correction**: The right to correct inaccuracies in your Personal Information.
- **The Right to Opt Out**: The right to opt out of targeted advertising, the sale of your Personal Information and profiling in furtherance of decisions that produce legal or similarly significant effects.

ii. Delaware and Maryland

- **Right of Access**: The right to confirm whether we process your Personal Information and request to access to such Personal Information.
- **Right to Deletion**: The right to request that we delete Personal Information we have collected about you.

- **Right to Data Portability**: The right to request that we provide you with your Personal Information in a portable format.

- **Right to Correction**: The right to correct inaccuracies in your Personal Information.

- **Right Regarding Third Party Disclosure**: The right to obtain a list of the categories of third parties to which we have disclosed your Personal Information.

- **The Right to Opt Out**: The right to opt out of targeted advertising, the sale of your Personal Information and profiling in furtherance of decisions that produce legal or similarly significant effects.

iii. Florida

- **Right of Access**: The right to confirm whether we process your Personal Information and request to access to such Personal Information.

- **Right to Deletion**: The right to request that we delete Personal Information we have collected about you.

- **Right to Data Portability**: The right to request that we provide you with your Personal Information in a portable format.

- **Right to Correction**: The right to correct inaccuracies in your Personal Information.

- **The Right to Opt Out**: The right to opt out of targeted advertising, the sale of your Personal Information and profiling in furtherance of decisions that produce legal or similarly significant effects; the collection of sensitive data including precise geolocation data; the processing of sensitive data; and the collection of personal data collected through the operation of a voice recognition or facial recognition feature.

iv. Oregon

- **Right of Access**: The right to confirm whether we process your Personal Information and request to access to such Personal Information. You may also obtain a list of specific third parties, other than natural persons, to which we have disclosed any Personal Information.

- **Right to Deletion**: The right to request that we delete Personal Information we have collected about you.

- **Right to Data Portability**: The right to request that we provide you with your Personal Information in a portable format.

- **Right to Correction**: The right to correct inaccuracies in your Personal Information.

- **The Right to Opt Out**: The right to opt out of targeted advertising, the sale of your Personal Information and profiling in furtherance of decisions that produce legal or similarly significant effects.

v. Minnesota

- **Right of Access**: The right to confirm whether we process your Personal Information and request to access to such Personal Information.

- **Right to Deletion**: The right to request that we delete Personal Information we have collected about you.

- **Right to Data Portability**: The right to request that we provide you with your Personal Information in a portable format.

- **Right to Correction**: The right to correct inaccuracies in your Personal Information.

- **Right to Opt Out**: The right to opt out of targeted advertising, the sale of your Personal Information and profiling in furtherance of decisions that produce legal or similarly significant effects.

- **Further Rights Concerning Profiling**: If we profile your Personal Information in furtherance of decisions that produce legal effects, you may have the right to question the result of the profiling, to be informed of the reason that the profiling resulted in the decision, and, if feasible, to be informed of what actions you

might have taken to secure a different decision and the actions that you might take to secure a different decision in the future. You have the right to review your Personal Information used in the profiling. If the decision is determined to have been based upon inaccurate personal data, you have the right to have the data corrected and the profiling decision reevaluated based upon the corrected data.

vi. Iowa

- **Right of Access**: The right to confirm whether we process your Personal Information and request to access to such Personal Information.
- **Right to Deletion**: You have the right to request that we delete Personal Information we have collected about you.
- **Right to Data Portability**: The right to request that we provide you with your Personal Information in a portable format.
- **The Right to Opt Out**: The right to opt out of the sale of your Personal Information.

vii. Utah

- **Right of Access**: The right to confirm whether we process your Personal Information and request to access to such Personal Information.
- **Right to Deletion**: The right to request that we delete Personal Information we have collected about you.
- **Right to Data Portability**: The right to request that we provide you with your Personal Information in a portable format.
- **Right to Opt Out**: The right to opt out of the processing of Personal Information for purposes of targeted advertising or the sale of your Personal Information

b. How to Exercise Your Rights

You may exercise your rights to request disclosure or deletion of Personal Information by submitting a verifiable request by one of the following methods:

- submitting a request online at https://datarequest.bsh-group.us/en/form?c=us
- emailing a request to bsh-us-dataprotection@bshg.com
- calling our toll-free number (855) 769-1755

If you email or call, please include your name, address, and phone number or email in all communications and state clearly the nature of your request.

We will respond to verifiable requests free of charge. If you are unhappy with the outcome of your request to exercise one of your rights, you may appeal our decision by emailing us at bsh-us-dataprotection@bshg.com. We may request you provide additional information if needed for your appeal.

With respect to your right to opt out, because we neither “sell” nor “share” Personal Information, we do not provide a mechanism to opt out of such disclosures.

c. Authorized Agent

Depending on your state of residence, you may have the right to designate an agent to exercise these rights on your behalf. We may require proof that you have designated the authorized agent to act on your behalf and to verify your identity directly with us. Please use this form or contact us at bsh-us-dataprotection@bshg.com for more information if you wish to submit a request through an authorized agent.

17. Contact Us

For questions on the topic of data protection, please contact us using the contact information provided in the App.

Communications about this Privacy Policy, as well as complaints concerning compliance with this Privacy Policy, may be directed to bsh-us-dataprotection@bshg.com. Complaints must be made in writing.

Within a reasonable time of receipt of your complaint, our Privacy Officer will investigate the complaint. The format of the investigation will vary depending on the circumstances. After the investigation, we may take measures to rectify the source of the complaint if required.

Last Updated: June 23, 2025