December 2025

DATA PROTECTION POLICY

Updated as of: 15.12.2025.

The data controllers of your data are the following companies:

- ConnectLife, data technologies, LLC Partizanska cesta 12, 3320 Velenje, Slovenia,
- Hisense UK ltd. Ground Floor, Munroe Court White Rose Office Park, Millshaw Park Lane, Leeds, LS11 0EA.

(hereinafter, both controllers referred to as the Company or Companies)

We treat your personal data seriously and responsibly with respect to the provisions of the Data Protection Act 2018, and other applicable regulations in the field of personal data protection. This document contains information on data processing activities we undertake related to the personal data of users of our products, our customers, potential customers, and/or website users. This document applies to data processing conducted on the websites of companies within Hisense Europe Group, within the ConnectLife application, and all other processing of personal data that you provide to any of the companies within the Hisense Europe Group.

In addition to the data protection policy:

- we adopted an internal procedure regarding the protection of personal data, in which the obligations of the Company and employees regarding the protection of personal data are determined.
- we adopted the Cookie Policy (https://uk.hisense.com/cookie-notice) which regulates the protection of the personal data of website users.
- we have created a dedicated e-mail box where you can contact us regarding all questions about your personal data.
- we regularly educate employees about the handling of personal data.
- we regularly check personal data handling systems and implement improvements.

December 2025

DATA PROTECTION POLICY 1
1. Who processes your personal data? 3
2. Method of obtaining data 3
3. Which of your personal data do we process and for what purpose? 3
a) Purchase on the Company's website or collection of the products ordered online 3
3.1. General customer support and customer support in troubleshooting and warranty claims 4
b) Product Safety and Recall Notifications 6
3.2. Notification related to products back in stock 6
3.3. User account on the Company's website or ConnectLife mobile app 7
3.4. Registration of the product at our website and ConnectLife mobile app . 8
3.5. Users' reviews, feedback, and opinions 9
3.6. Notifications, personalized offers via digital channels, and related services 11
3.7. Information about your activities on our website 12
3.8. Processing of personal data via social networks, instant messaging applications and chat rooms 13
3.10 Use of products through the ConnectLife applications 14
3.11. Cookies and other online tools 17
3.12. Remarketing, tracking, and similar technologies 18
3.13. Video Surveillance 19
4. Use of Artificial Intelligence (AI) 19
5. Collection of children's personal data 20
6. Profiling 20
7. The existence of automated decision-making 20
8. How do we protect your personal data? 21
9. Retention 21
10. Who processes your personal data and with whom do we share it? 21
11. Where do we store your data? 25
12. Notice to residents of certain states in the United States 25
13. Notice to residents of Canada 28
14. Notice to residents of Mexico 30
15. Do not track settings 31
16. What are your rights and how to exercise them 31
17. Data Protection Officer 32
18. Compliance with the EU Data Act 32
19. Data Protection Policy Versions and Changes 32

December 2025

1. Who processes your personal data?

The controllers of your personal data are:

Company: ConnectLife, data technologies, LLC
Address: Partizanska cesta 12, 3320 Velenje, Slovenia
e-mail: privacy@connectlife.io

Company: Hisense UK
Address: Ground Floor, Munroe Court White Rose Office Park, Millshaw Park Lane, Leeds, LS11 0EA.

Other companies within Hisense Europe Group may be processors of your personal data. As such, the companies of Hisense Europe Group are collecting and in other ways processing your personal data. Their means of data processing (e.g. websites, CRM programs, online tools, etc) are for the purpose of this policy stated as our means. The list of other companies of Hisense Europe Group, and their external contractors is available here link.

2. Method of obtaining data

We obtain your personal data when you buy our products, use our websites or applications, through cookies and other online tools, fill out forms on our website or in physical form, through telephone and electronic communication, through other written communication, and/or through social networks.

3. Which of your personal data do we process and for what purpose?

In this section, we explain which data we process, for what purpose, and based on which legal basis, all depending on the individual's activity and use of our products and services.

Besides the purposes stated below we can process all below-stated data to the extent absolutely necessary and proportionate to ensure the security of information networks, information systems and information, where this processing is based on the legitimate interest of the Company. This helps us monitor, prevent and detect fraud and abusive use of our services, websites and systems, enhance system security, and combat spam, malware, malicious activities or other security risks.

a) Purchase on the Company's website or collection of the products ordered online

In order to purchase products via the Company's website or to collect products ordered online, we must collect and process some of your personal data (e.g. delivery address), as this is the only way we will be able to process your order.

To enable a purchase on the Company's website or collection of products ordered online, we will process the following data:

- customer ID,
- first name and last surname,
- language of communication,
- invoicing address and delivery address (if the delivery option is selected),
- e-mail address,
- phone number,
- order (number, value)
- method of payment,
- bank account number and/or credit card number,
- product type, model, and number
- serial number of the product
- purchase invoice
- purchase history

The purpose and basis of the processing of the above data is to ensure the possibility of delivery or acceptance of the order, payment of the order, information about the status of your order and issuance of an invoice for the completed purchase. By placing an order, you have made a purchase, which legally means that you have entered into a sales contract, and to fulfill obligations arising for us from the sales contract, we must process your personal data (processing is necessary for the performance of a contract), and at the same time, we are obliged by law to issue an invoice for the completed purchase (processing is necessary for compliance with a legal obligation).
After your purchase, and based on our legitimate interest in ensuring you can fully benefit from your device, we will process your e-mail address to inform you about the option to connect your device to the ConnectLife mobile app. This app allows you to use your device more conveniently, access all relevant documents in one place, and enjoy additional functionalities. The notification will be sent a maximum of two times, shortly after your purchase.

Processing period: Data related to the purchase itself is stored as long as you can exercise certain rights in connection with your purchase according to the competent law (the period outlined in the law in which it is possible to lodge the claim with a competent court – usually the general limitation period prescribed by the applicable legislation). Per tax and accounting regulations, data for issuing invoices are kept for the mandatory period prescribed by local legislation.

What happens if you do not provide personal data? In the case of online shopping or collecting the products ordered online, we cannot carry out your purchase or collection of the products without obtaining above listed personal data. Still, you can buy and collect the products directly in our physical store or in the stores of contractual partners that enable the latter.

3.1. General customer support and customer support in troubleshooting and warranty claims

In order to provide general customer support (responding to inquiries of customers and potential customers) and customer support for troubleshooting and warranty claims, we need to collect and process some of your personal data, as this is the only way we can respond to your inquiries or meet our legal obligations in this regard.

In order to provide general customer support and customer support for troubleshooting and warranty claims, we may process the following data:

- name and surname,
- e-mail address,
- phone number,
- order number,
- purchase invoice,
- address,
- language of communication,
- date of claim,
- service history,
- duration of warranty and extended warranty,
- type of warranty,
- warranty related only to specific parts of the product,
- e-mail communication
- chat transcript
- video conference recording (in case of video conference) (subject to consent, where applicable)
- pictures (in case the user sends us pictures of the product)
- in the case of a call to the call center, a recording of the telephone call (subject to consent, where applicable).

In case where customer support for troubleshooting and warranty claims is related to smart devices, please also check chapter 3.10. of this document.

The purpose and basis of processing the above data is responding to inquiries of customers and potential customers (processing is based on our legitimate interest) or compliance with the legal provisions regarding the seller's warranty for the purchased products (processing is necessary for compliance with a legal obligation) and the fulfillment of the purchase agreement regarding the purchased products (processing is necessary for the performance of a contract). Within customer support for troubleshooting and warranty claims we may (based on your consent) also use Visual Remote Assistant (software that enables real-time communication between a remote expert and an onsite customer via audio-video streaming and augmented reality tools). Additionally, in case of a telephone call with our customer care center, we may record your call. Sometimes we will base this recording on our legitimate interest to train our agents and improve our customer care services, but sometimes we will base this recording on your explicit consent (when local legislation requires so).

Processing period: Data is kept for the duration of the possibility of asserting claims from the correspondence, contract, and warranty according to the competent law (period outlined in the law in which it is possible to lodge the claim with a competent court - usually the general limitation period prescribed by the applicable legislation). Phone call recordings are kept for a period of three months (or until the consent is revoked, if applicable). Personal data for use of Visual Remote Assistant are stored until the consent is revoked where you can withdraw your consent at any time. The data will cease to be stored within 1 month of receiving the revocation of the consent.

What happens if you do not provide personal data? Non-providing the above listed personal data may affect the provision and quality of customer support regarding

the use of our products, or the way of resolving warranty claims. However, depending on the channel and reason of communication we may not need all the above listed data.

b) Product Safety and Recall Notifications

For the safety and proper functioning of your device, we may need to contact you if a manufacturing defect or malfunction is identified that could affect your product's performance or safety. This may include situations where a product recall is required. We may use your contact information that we obtained from various entry points before, such as:

- e-mail address,
- phone number,
- postal address.

The purpose and basis: We will use your contact information available to us at the time to inform you about potential safety issues or defects related to the product you purchased, provide instructions on corrective actions, replacements, or recalls, and ensure you receive timely updates to protect your safety and maintain device functionality. Processing your contact information for this purpose is based on our legitimate interest in ensuring the safety of our products and protecting our customers, in line with applicable data protection laws.

Processing period: The processing period is the same as described in other sections of this Policy for when contact information is collected. In the rare event that a product recall is needed or product safety is compromised, we will use only the contact information we have available at that time to notify affected users.

What happens if you do not provide personal data? If we do not have your contact information, there is no need to worry. Any necessary actions will also be publicly announced. However, direct contact with customers is always more efficient and faster in such situations.

3.2. Notification related to products back in stock

In the event when a certain product is out of stock individual can insert his or her email in order to be notified when the product is back in stock.

In order to notify individual about the availability of the product we will process the following data:

- e-mail address.

The purpose and basis of the processing of your personal data is to notify you about the availability of the product. The processing of personal data is carried out only based on your consent.

Processing period: Until the consent is revoked where you can withdraw your consent at any time. The data will cease to be stored within 1 month of receiving the revocation of the consent or within 1 month after the notification about the availability of the product is sent to the individual.

What happens if you do not provide personal data? In case of non-providing your e-mail address we cannot notify you about product back in stock, however for the same purpose you may check our website regularly.

3.3. User account on the Company's website or ConnectLife mobile app

Any individual can create a user account on the website or within ConnectLife mobile app. A user account is intended to monitor the progress of the order, view the purchase history, give an opinion about the product, get user manuals and product information, use all functions of smart devices, etc. Within the settings of the user account, it is also possible to express the will to receive marketing messages or to cancel receiving them.

In order to create a user account, we may process the following data:

- user ID
- e-mail address
- name and surname,
- phone number,
- address,
- language of communication,
- password,
- food preferences,
- purchase invoice,
- service ticket and service history,
- social network login (in case of establishing user account with social media account: e-mail address, first name, last name, language of communication, photo URL, provider, provider ID),
- account information (login enabled, log, profile update, login location, account created, account access log)
- password (last login, disable login).

The purpose and basis of the processing of your personal data is to ensure access to your account and user authentication. With the request to create a user account, a contractual relationship has been established, and in order to fulfil our part of the contractual obligations, we will process your personal data (processing is necessary for the performance of a contract). In case of uploading the purchase invoice please be aware that the invoice is linked to the device and the content may be visible to other users that pair with this device. Some of the personal data (service ticket and service history) are processed in order to fulfil our obligations arising from the purchase agreement regarding the purchased products (processing is necessary for the performance of a contract).

Processing period: We keep your personal data until you delete your account or up to 3 years after the last login to the account. Data processed based on the contract are kept for the duration of the possibility of asserting claims from the contract according to the competent law (period set forth in the law in which it is possible to lodge the claim with a competent court). Personal data that are processed based on your consent are kept until the consent is revoked and you can withdraw your consent at any time. Those data will cease to be stored within 1 month of receiving the revocation of the consent, where in that time period you may still be recipient of our communication.

What happens if you do not provide personal data? It is not possible to create a user account without the above determined personal data. Still, you are not obliged to create a user account (i.e. to provide personal data for such a purpose) to purchase or use our products.

3.4. Registration of the product at our website and ConnectLife mobile app

For certain products and on certain markets buyers of our products can register the product at our website or through ConnectLife mobile app within his or her user account. Based on registration the individual may (for certain products) acquire simplified access to the instructions for use, our proposals on how to use our products, information related to warranty, for certain products additionally extended period of warranty and notifications about updates related to ConnectLife appliances. For certain products and in limited period of time within the promotion organised via marketing agency, it is possible also to get partially refund of the purchase price in case of registration of the product at our website or ConnectLife mobile app.

It is possible to register a product produced by us, but sold under a brand different from the brands listed in Section 1. of this Policy. If this is the case, please note that there is another data protection policy that applies to the processing of personal data for registration of the product, not this one.

In order to perform registration of the product, we will (besides the data stated in point 3.4.) process the following data:

- product number,
- serial number of the product,
- date of purchase,
- copy of the purchase invoice.
- IBAN number (only for the purpose of partial refund of the purchase price)

The purpose and basis of the processing of your personal data is to enable extended warranty (only related to certain products), provide even easier access to the instructions for use and our proposals on how to use the product. By registration of the product, you accept the rules of the registration that is legally treated as contractual relationship and in order to fulfil our part of the contractual obligations, we will process your personal data (processing is necessary for the performance of a contract).

Processing period: We keep your personal data until you delete your registration of the product, while we keep data related to the extended warranty for the duration of the possibility of asserting claims from the contract according to the competent law (period set forth in the law in which it is possible to lodge the claim with a competent court).

What happens if you do not provide personal data? Without above stated data you cannot register the product at our website or Connectlife mobile app. However, each product has at the time of the purchase attached instructions for use and information related to warranty.

3.5. Users' reviews, feedback, and opinions

a) Providing users' reviews on the website and users' feedback related to our products and services

In order to enable the possibility of providing user's reviews (evaluations, opinions, ratings and comments) on the website, we must collect and process some of your personal data, as we want to share the experiences of actual customers and users with potential customers and users. We may share experiences of actual customers and users of certain product or service from one market also with potential customers and users in other market.

In order to receive users feedback related to our product and services we may contact you after the product was delivered to you or the service was performed, where providing your feedback is voluntarily.
In order to provide user's reviews (opinions, ratings and comments) or to acquire users feedback, we will process the following data:

- name or chosen name or review as a guest,
- e-mail address,
- details of purchased products or service performed,
- copy of the purchase invoice
- rating or comment
- review language
- our response
- sentiment analytics of user product reviews.

The purpose and basis of the processing of your personal data is to ensure that the user review of the individual product was given by the person who actually purchased or uses the individual product. The processing of personal data may be carried out based on your consent, while acquiring user feedback related to our product and services within 30 days after the delivery of the product or service performed is based on our legitimate interest which is in this case product improvement, quality assurance and customer satisfaction evaluation.

Processing period: Your personal data will be automatically deleted from our servers, workstations and systems (please see section 9 below) or anonymized after 5 years after publishing the user's review. Your opinions, ratings and comments are visible on the website for 5 years after publishing on the website. However, your user review or user feedback will be deleted or anonymized earlier in case of request for erasure or withdrawal of your consent to such data processing, where in those cases the data will cease to be stored within 1 month of receiving the revocation of the consent. Please note that deleting personal data in accordance with this section of the Policy does not mean that your personal data will also be simultaneously deleted or anonymized from the databases of third parties who manage the social network, i.e. the platform through which you left your opinion, rating or comment. Deletion of personal data from such third parties' databases is governed by each such third party's specific privacy policy, not this one. We do not control these third parties and therefore recommend that you review their privacy policies to understand how they process and when they delete or anonymize your personal data. The personal data we process for contacting users in

order to acquire their feedback will be automatically deleted or anonymized within 30 days after the delivery of the product or the performance of the service.

What happens if you do not provide personal data? You may provide the user's review also anonymously (without providing your personal data). However, without your personal data we may not ensure that opinions, ratings and comments are given only from actual purchasers and users.

b) Improving our products and services by obtaining users' opinions on the general use of such products and services (regardless of the brand)

To find out what problems users encounter when using products and services of the same type that we sell or provide, we ask users of these products and services in general (regardless of the brand) about their overall experience with such products or services by sending them a questionnaire. This helps us to understand the needs of the market better and improve our products and services in line with users' opinions/habits/preferences.

In order to acquire users' opinions on the use of the products and services of the same type as the one we sell/provide, we will process the following data:

- e-mail address
- type of the product they use
- brand of the product they use
- details on users' satisfaction with the products they own.

The purpose and basis of the processing of your personal data is to improve our products and services by adjusting them to the needs and experiences of actual users of such products and services in general (regardless of the brand). The processing is based solely on your explicit consent to receive such questionnaires at your e-mail address while answering the questions contained in such questionnaires is voluntary.

Processing period: The personal data we process for sending questionnaires to users of products and services of the same type as the products and services we offer/provide, will be processed for as long as you do not withdraw your consent to such data processing, where in those cases the data will cease to be stored within 1 month of receiving the revocation of the consent. The personal data contained in the completed questionnaires will be deleted from our servers, workstations, and systems (please see section 9 below) or anonymized 5 years after you send us the completed questionnaire. Please note that deleting personal data in accordance with this section of the Policy does not mean that your personal data will also be simultaneously deleted or anonymized from the databases of third parties who may manage the platform through which you left the completed questionnaire (if applicable). Deletion of personal data from such third parties' databases is governed by each such third party's specific privacy policy, not this one. We do not control these third parties and therefore recommend that you review their privacy policies to understand how they process and when they delete or anonymize your personal data.

What happens if you do not provide personal data? If you do not provide your personal data, i.e. give consent to receive such questionnaires at your e-mail address,

you will not receive them. Even if you receive such questionnaires, completing them is voluntary.

3.6. Notifications, personalized offers via digital channels, and related services

a) Sending newsletters, personalized offers, abandoned cart reminders, and invitations to participate in prize games

For the purpose of marketing activities and providing information about our products (e.g. sending newsletters, personalized offers, abandoned cart reminders, invitations to participate in prize games, etc.), we need your express consent (divided into specific purpose) and without the latter, we will not contact you for the purpose above. As a channel of communication, we can in case of your consent use e-mail, social media, ConnectLife mobile app, or other instant messaging applications. We will send you personalized offers (where we can recommend content through ads and notifications) and abandoned cart reminders (where we send you an e-mail with the items you left in the cart), only if you previously gave your consent for receiving personalized offers. Sometimes, for sending personalized offers, we may use profiling as described within this privacy policy (see Section 5). You can always revoke your given consent in your user account settings, by unsubscribing from receiving messages, blocking us on social media or within instant messaging applications, changing cookie settings, or sending us a request to privacy@connectlife.io.

For the purpose of sending notifications, abandoned cart reminders, personalized offers via digital channels and related services, we may process the following data:

- name and surname,
- e-mail address,
- phone number,
- data related to prize games (model, serial number, purchase date, invoice)
- photo material and video recordings
- location data of the user obtained from the user's mobile device,
- the individual's interests regarding viewing products on websites,
- contact information via instant messaging applications,
- purchase history,
- postal code,
- data related to delivery, opening, clicking and unsubscriptions of our messages,
- sentiment analytics of user product reviews.

The purpose and basis of the processing of your personal data is to enable the sending of marketing messages, abandoned cart reminders, to present a personalized offer based on your interests, to publish videos featuring you on our official digital channels or to improve your user experience. The processing of personal data is carried out only based on your consent.

Processing period: Until the consent is revoked where you can withdraw your consent at any time. The data will cease to be stored within 1 month of receiving the revocation of the consent where in that time period you may still be recipient of our communication.

What happens if you do not provide personal data? You are not obliged to provide your personal data for marketing purposes (providing consent for personal data processing for these purposes is voluntary). Still, in such a case we will not be able to notify you about our marketing activities, and our products and create personalized offers for you.

b) Sending push notifications within ConnectLife mobile app

To send push notification within ConnectLife mobile app designed for in-app promotions, in-app guidance and personalised marketing promotions we need your express consent and without the latter, we will not contact you for the purpose above.

In order to send you push notification within ConnectLife mobile app, we will process the following data:

- email address
- language of communication
- device and the IP address
- geolocation (country, state, and city)
- device token or unique identifier (assigned by your device's operating system to enable notifications)
- ConnectLife mobile app interaction data
- appliance interaction data (see point 3.10 of this policy)
- details of purchased products,
- date of purchase,
- date of claim,
- service history.

The purpose and basis of the processing of your personal data is to enable the sending of push notifications within ConnectLife mobile app. The processing of personal data is carried out only based on your consent.

Processing period: Until the consent is revoked where you can withdraw your consent at any time. You can disable push notifications at any time through the notification settings in the ConnectLife mobile app or through your smart device's operating system settings. The data will cease to be stored within 1 month of receiving the revocation of the consent where in that time period you may still be recipient of our communication.

What happens if you do not provide personal data? You are not obliged to provide your personal data for sending push notifications within ConnectLife mobile app (providing consent for personal data processing for these purposes is voluntary). Still, in such a case we will not be able to send you push notifications within ConnectLife mobile app.

3.7. Information about your activities on our website

For the purpose of improving the functioning of the website, statistical reviews and personalized offers, we also monitor your activities on our website, whereby this data is in anonymized form.

For the purpose of monitoring the activity on our website, we process the following data:

- user account designation,
- purchase history,
- device operating system,
- used browser,
- web address (URL address) of the initial page that you use to access to our website.

The purpose and basis of the processing is to improve the functioning of the website, and statistical reviews. We use cookies and similar tracking technologies to track the activity on our website, where the use of cookies is allowed only based on your consent. Based on the use of cookies we can use those data for personalized offers but only in case when we acquire additional consent for the latter. You can always revoke your given consent in your user account settings, by changing cookie settings or by sending us a request to privacy@connectlife.io.

Processing period: Your personal data acquired by cookies will be automatically deleted or anonymized after the duration of specific cookies (as defined in cookie policy), while your data used for personalized offers will be deleted or anonymized in case of revocation of the consent where in those time period you may still be recipient of our communication.

What happens if you do not provide personal data? In case you do not provide above stated data (by consent to cookie policy) we cannot track your activity on our website, improve the functionality of our website, and prepare personalized offers for you.

3.8. Processing of personal data via social networks, instant messaging applications and chat rooms

The company may have established profiles on social networks (e.g. LinkedIn, Instagram, Facebook, TikTok, Twitter, etc.) or may use instant messaging applications (e.g. WhatsApp, FB Messenger, Viber, etc.) for communication. Social networks and instant messaging applications allow us to promote our products and services or provide customer support. When doing the latter, we can also select categories of individuals on the social network to which we want our promotions to refer (in case of specific consent acquired). As such, the Company may be responsible for the protection of personal data that users share with the Company through the aforementioned media, and at the same time, the provider of the individual media is also responsible for the data processing it performs on such media, so users are advised to familiarize themselves with the privacy policy of the individual media.

In the case of visiting the Company's profile on an individual social network or establishing communication via instant messaging applications, we can process the following data:

- if you like, share a post, mark the Company's profile or comment, we receive access to your public profile and the content of your post,

- if you send us a private message on a social network or through an instant messaging application, we obtain information about your public profile, or your contact information and information about the content of the sent message.

When communicating via social networks, instant messaging applications and chat rooms, we will process the following data about you:

- the public profile of the individual on the social network and the content of the publication,
- contact information of the individual in the instant messaging application,
- other data that you will provide to us during the communication.

The purpose and basis of the processing of your personal data is the promotion of the Company's products and the establishment of communication with users of social networks or instant messaging applications. We may contact you only based on your consent, but we can respond to your inquiry based on our legitimate interest, which is satisfying the needs of customers by providing information related to our products.

Processing period: Your personal data kept by us will be automatically deleted or anonymized after 1 year since the communication occurred or earlier in case of withdrawing your consent. In case of withdrawing the consent, the data will cease to be stored within 1 month of receiving the revocation of the consent where in that time period we may still process your personal data.

What happens if you do not provide personal data? Without providing your personal data you cannot communicate with us through the aforementioned media, and we cannot respond to your inquiries.

3.10 Use of products through the ConnectLife applications

For the purpose of using all functions of smart devices and services through the application, service and troubleshooting services for smart devices, improving our offer of devices and services, for the purpose of notification in case of safety instructions (including also any updates available and recommendations for extending the lifecycle of the product) and/or information about the recall of devices, we collect and process some of your personal data and device performance data.

Use of products through the Connectlife applications is possible only in case of user registration and the conclusion of a license agreement.

For user registration and the conclusion of the license agreement, we will process the following personal data:

- name and surname,
- language of communication,
- address,
- phone number,
- e-mail address.

During the usage of the device (and depending on the type of device), we will perform data analysis related to the usage of the device. For this purpose, we will process the following data:

- appliance's data (brand, model, serial number),
- appliance unique identifier (AUID),
- installation date of the device,
- data on pairing the device with our cloud (appliance paired, pairing type and timestamp)
- operation of the appliance (commands sent to appliance, appliance settings, status and statistics, notifications, appliance alarms and errors, service ticket requests, timer and automation)
- data detected by the device's sensors and which are important for the operation of the device (e.g. data regarding technical performance, data related to possible error messages, temperature, humidity, air quality, etc.),
- booking log (for public laundry)
- food images from appliances and time-lapse videos (in case where those materials contain an image of any person you are obliged to receive their consent for this purpose)
- user behavior analytics,
- device booking,
- resource (water, electricity) consumption,
- food and drink storage and preferences– when a recipe is selected, the app will show which ingredients are already in the user's storage, making meal planning easier,
- appliance and user's location data (and nearby providers of services and goods).

If you allow another user (regardless of whether through your account or his own account) to use devices through the application, data about the use of devices created by the additional user will also be stored, whereas in the case where you allow other user to use your account, we are not able to differ between different users of the same account and all personal data will be linked to initial user. However, initial user is obliged to inform other users of the same account about the stated fact and the content of this policy and license agreement.

In order to connect the appliance to the cloud via local WIFI users have to insert also data about Service Set IDentifier (SSID) and a password. However, those data are used only for pairing the appliance with the Wi-Fi module and will be processed until the user cancels the device distribution network.

In case of acquiring your specific consent, we may use those data also for non-contractual purposes (recommendations for use of device, direct marketing and personalized offer) where we can recommend content through ads and notifications.

If you activate the voice control functionality by connecting your appliance to a third-party voice assistant (e.g., Amazon Alexa or Google Assistant) in order to enable device control through the voice assistant, the following categories of data may be processed:

- Device ID and configuration
- Appliance usage status (on/off, mode, etc.)
- Commands sent through the voice assistant (e.g., "Turn on the dishwasher")

- Time and frequency of use
- Your associated user account

To enable voice control, your device shares limited technical data with the voice assistant provider (e.g., Amazon or Google), and these providers process data in accordance with their own privacy policies. We do not record or process your voice data directly. That processing is done exclusively by the voice assistant provider.

The basis for processing personal data related to the use of a voice assistant is your consent, where you can always revoke your given consent in your user account settings, or by sending us a request to privacy@connectlife.io. Integration with voice assistants is entirely optional. You can use the appliance without enabling this functionality.

In addition to the purposes stated above, we may use non-personal data related to the usage of our appliances for internal statistical analysis. For information on the use of non-personal data in the context of the EU Data Act, effective from 12 September 2025, please refer to the EU Data Act User Data Notification available here: EU Data Act User Data Notification V2.0 - ConnectLife
The purpose of the processing of your personal data is stated above, where the **basis** is different related to each specific purpose.

The basis for processing personal data related to use of all functions of smart devices and services through the application and for service and troubleshooting services for smart devices is the contractual relationship based on concluded sales contract and license agreement and in order to fulfil our part of the contractual obligations, we must process your personal data for contractual purposes.

The basis for using personal data related to the improvement of our offer of devices and services are legitimate interests where we as a controller are constantly striving for improvement of our offer of devices and services.

The basis for using personal data related to notifications in case of safety instructions and/or information about the recall of devices are our legal obligations related to the safety of our devices and processing is necessary in order to protect your vital interests.

The basis for using personal data related to non-contractual purposes (recommendations for use of device, direct marketing and personalized offer) is your specific consent, where you can always revoke your given consent in your user account settings, or by turning off the notification option within the application or by sending us a request to privacy@connectlife.io.

Processing period: Above stated data are stored as long as you can exercise certain rights in connection with our contractual obligations (period set forth in the law in which it is possible to lodge the claim with a competent court after the expiry of the license agreement) or until you delete your account or up to 3 years after the last login to the account.
During your use of the application, we will continue to save your personal data. If you no longer use the application, you can click the “Delete Account” button through the application or in some cases by disconnecting the appliance and using it “offline”. After

you confirm the deletion of your account we will clear your personal data left in the application.
You can also click on the "Settings" button in the top right corner of the dropdown menu in the application to enter the "Settings" page. Then click to open the "System" page. Enter the "Reset" item, and you yourself can start the reset process. After the reset process is completed, the user data stored on the device will be deleted.
If you have allowed the use of the device together with another user of the application who does not use his account, the deletion of your account also triggers the deletion of the other user. If you have allowed the device to be used together with another user of the application using his account, please note that deleting your account does not trigger the simultaneous deletion of the additional user.

Data related to **non-contractual purposes (recommendations for use of device, direct marketing and personalized offer)** are stored until the consent is revoked where you can withdraw your consent at any time by sending us a request to privacy@connectlife.io. or until you delete your account where you can delete it at any time. The data will cease to be stored within 1 month of receiving the revocation of the consent or within 1 month since account deletion (as the case may be), where in those time period you may still be recipient of our communication.

What happens if you do not provide personal data? It is not possible to register a user of the ConnectLife application and conclude a license agreement without above stated personal data. However, you may still use the basic functions of our devices (without smart functionalities) in case of non-concluding a license agreement.

3.11. Cookies and other online tools

If you visit our web page, we may store cookies on your device. For more information on cookies used on our webpage, please see the Cookie Policy (https://uk.hisense.com/external-privacy-notice).

In addition to cookies, we also use other online tools from the following providers:

Google, namely:

- Google Marketing Platform for the purpose of obtaining data related to website traffic (e.g. number of visitors, pages visited by visitors, time spent by visitors on the website);
- Google Maps for the purpose of using the mapping service Google Maps via API in order to facilitate the location of places specified by the individual on the website;
- Google Tag Manager for the purpose of managing website tags through the user interface and integration of program codes on our websites;
- Google Ads for the purpose of placing advertisements, remarketing and tracking conversions;
- Google Optimize for the purpose of A/B testing and website testing;
- Site Kit for the purpose of improving and monetizing our content on the web page;
- Youtube for the purpose of establishing a connection with YouTube servers, where the use of plugins from YouTube is required;

- Google Analytics for the purpose of collecting data from websites and apps to create reports that provide business insights;
- Google Search Console in order to show the performance of websites on Google Search and how Google sees our website
- Looker Studio for the purpose of turning data into informative, easy to read, easy to share, and fully customizable dashboards and reports.

The listed online tools are operated by Google Ireland Limited, whereby certain information about an individual's use of the website may also be transferred to a server in the USA, so we suggest that you also familiarize with their privacy policy, which is available here: LINK. If you are a Google Account holder and have consented to the customization of ads, we may also obtain reports on the effectiveness of our advertising measures (including cross-device reports), demographic information and interests of individuals, as well as cross-device online advertising functions.

Meta, namely:

- Meta business suite as a social media management tool for Facebook and Instagram for the purpose of creating and scheduling content to responding to engagement to analyze insights
- Meta pixel for the purpose of placing advertisements, remarketing and tracking conversions.

The listed online tools are operated by Facebook Ireland Limited, with a registered office at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, D02 X525, Ireland; whereby certain information about an individual's use of the website may also be transferred to a server in the USA, so we suggest that you also familiarize with their privacy policy, which is available here: LINK. If you are a Facebook or Instagram account holder and have consented to the customization of ads, we may also obtain reports on the effectiveness of our advertising measures (including cross-device reports), demographic information and interests of individuals, as well as cross-device online advertising functions.

3.12. Remarketing, tracking, and similar technologies

We and our third-party service providers use cookies to inform, optimize and serve ads based on your past visits to our web page or our mobile apps in order to advertise on third-party websites to you. For this purpose we use:

- Google Ads, provided by Google and you can opt-out of this by visiting the Google Ads Settings page: https://adssettings.google.com/authenticated, and
- Facebook Retargeting, provided by Meta and you can opt-out this by visiting the Facebook site where you have to log in and go to *Settings* > *Ads* > *Ad Settings*. On the app, go to *Setting & Privacy* > *Settings* > *Ad* > *Ad Preferences* > *Ad Settings*. Then choose the *Not Allowed*

To see how our web page and mobile app is performing we use conversion beacons, tags, scripts and pixels, that perform a short line of code to tell us when you have clicked on a particular button or reached a particular page. The use of these technologies allows us to record that a particular device, browser, or application has visited a particular webpage.

If you enable location-based services on your computer or mobile device in connection with your use of the web page or mobile app, you expressly consent to us collecting the geolocation (which may include specific longitude and latitude) of your device. This information will be used as set forth in this Data Protection Policy, including to provide specific advertising content or messages based on your location.

We and our third-party service providers may use the information that we collect about you (information from our web page or mobile app, through your device(s), or from a third party) to help us and our third-party service providers identify other devices that you use (e.g., a mobile phone, tablet, other computer, etc.). We, and our third-party service providers also may use the cross-device use and other information we learn about you to serve targeted advertising on your devices and to send you emails. These third-party cookies and other technologies are governed by each third party's specific privacy policy, not this one. We do not control these third parties and therefore recommend that you review their privacy policies to understand how they process your personal data.

3.13. Video Surveillance

When visiting some of our stores, your personal data may be processed through our video surveillance (CCTV) system. The CCTV system is in place to protect store property and ensure the safety and security of customers, employees, and other individuals on the premises.

Categories of personal data processed:

- CCTV footage (video recordings without sound)

The purpose and basis of processing CCTV footage is carried out for the legitimate interest of ensuring the security of persons and property, preventing theft, vandalism, and other security incidents.

Processing Period: CCTV footage is retained for a maximum of 30 days unless a longer retention period is required for the investigation of an incident or for the establishment, exercise, or defend legal claims.

What Happens if You Do Not Provide Personal Data? As CCTV operates automatically in our stores, it is not possible to opt out of this processing when entering the monitored areas. If you do not wish to be recorded, we recommend avoiding entry into those areas, which are clearly marked with CCTV signage in accordance with legal requirements.

4. Use of Artificial Intelligence (AI)

We may use Artificial Intelligence ("AI") technologies to assist users and customers, improve efficiency, and provide support. Examples of AI usage include AI chatbots that help with customer inquiries, AI troubleshooting features that suggest potential solutions to common technical or operational issues, and AI-generated recipes in the ConnectLife app, which provide recipe suggestions based on user-selected ingredients from a predefined list. These recipe suggestions are for informational purposes only;

users remain responsible for evaluating them, particularly regarding allergies or dietary restrictions.

AI features are used for assistance and informational purposes only and do not make automated decisions that affect the rights or obligations of users or customers. AI features do not use personal data to train or improve the model, and any personal data processed by AI is used temporarily to generate outputs and is not stored for model training purposes.

AI outputs are provided "as is" and may contain inaccuracies or incomplete information. While AI is intended to assist and improve efficiency, we cannot guarantee the accuracy, completeness, or suitability of AI-generated content for any purpose. Users and customers remain responsible for verifying outputs before acting on them.

Whenever AI outputs could affect legal rights, claims, or requests, a human reviewer or processor will always handle the final decision or action, ensuring compliance with GDPR principles regarding meaningful human intervention.

5. Collection of children's personal data

We are committed to protect the personal data of children and recognize that parents or legal guardians may use our services or purchase our products for family use, including by minors. As such, our services and products are not intended for use by individuals under the local adult legal age minimum, and we will not knowingly collect personal data from individuals under such age for any purpose, nor will we accept registration from such individuals. In some cases, particularly where information is collected electronically, we may not be able to determine whether information was collected from children under local legal age, and we treat such information as though it were provided by an adult. If we learn that a child under the local legal age has provided any personal data, we will use commercially reasonable efforts to delete or anonymize such information immediately.

6. Profiling

Profiling means any form of automated processing of personal data that involves the use of personal data to evaluate certain personal aspects relating to an individual, in particular to analyze or predict the personal taste, interests, behavior or location of that individual.

The company performs profiling if you have given your specific consent for personalized offers. Profiling is carried out using various methods of statistics, mathematics or predictive analysis, which allows us to predict your needs and prepare suitable offers based on this. As part of profiling, we analyze your demographic data, such as location, and data on purchases and device usage, on the basis of which we place you in an individual profile and only send you offers that we believe match your needs and habits.

7. The existence of automated decision-making

We do not process your personal data using means for automated decision-making that could have legal consequences for you.

8. How do we protect your personal data?

In order to protect your personal data, we have introduced a number of technical and organizational measures, namely:

- Measures for ensuring ongoing confidentiality, integrity, availability and resilience of processing systems and services
- Measures for ensuring the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Processes for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures in order to ensure the security of the processing
- Measures for user identification and authorisation
- Measures for the protection of data during transmission
- Measures for the protection of data during storage
- Measures for ensuring physical security of locations at which personal data are processed
- Measures for ensuring events logging
- Measures for internal IT and IT security governance and management
- Measures for ensuring data minimisation, data quality and limited data retention
- Measures for allowing data portability and ensuring erasure

9. Retention

We store your personal data within the period of your valid consent or the period under the contract between you and us, extended for the duration of the general limitation period prescribed by the applicable legislation unless there are other different requirements according to applicable laws. We will retain and use your personal data to the extent necessary to comply with our legal obligations (for example, if we are required to retain your data or the information you provided to us to comply with applicable laws), resolve disputes, and enforce our legal agreements and policies. We will retain your marketing contact information until you unsubscribe from our marketing communications. We will also retain website, applications and appliance usage data for internal analysis purposes, in line with the applicable legislation.

10. Who processes your personal data and with whom do we share it?

Your data is processed either within internal software programs (e.g. SAG and Hisense CRM) or with the use of tools provided by external providers (SAP CDC, Hybris, Salesforce, Mailchimp, SiteKit).

Other related entities of Hisense may have access to your personal data, as individual companies are sellers or manufacturers of the product you purchased, and individual companies provide adequate support for the Company's operations. Related entities of Hisense seated outside of EU/EEA appointed company VERDATA Datenschutz GmbH & Co. KG, Roemerstr. 12, D – 40476 Duesseldorf, Germany as their representative according to Article 27 of GDPR. Access to your personal data may have, in particular, the following related entities of the company Hisense:

- Gorenje, d.o.o., Partizanska cesta 12, 3320 Velenje, Slovenia
- Hisense International Co., Ltd, No.17, Donghai Xi Road, Qingdao, P.R.China.

Wherever the purpose can be achieved, transferred personal data is pseudonymized to enhance security and protect individual privacy. In addition, **Standard Contractual Clauses** and a **Transfer Impact Assessment** are implemented to ensure that all transfers comply with applicable data protection requirements.
The Company may also transfer personal data to external contractors (mainly for the purpose of ensuring payments, transportation, and other matters related to your order etc.). In such a case, the Company undertakes to enter into an agreement with the external contractors that ensures adequate security of your personal data, and the external contractors can process your data only for the purpose for which they were obtained.
The Company may also disclose personal data to a buyer or other successor in the event of a merger, divestiture, restructuring, reorganization, dissolution, or sale or transfer of some or all of our assets, whether as a going concern or as part of bankruptcy, liquidation, or similar proceeding, in which personal data held by us about our products and services users is among the assets transferred.
Your personal data may also be the subject of transfer to external contractors in third countries. In this case the Company will ensure adequate safeguards if the external contractors are seated or provide services relevant to the protection of personal data in a third country that does not offer the same level of data protection as GDPR and undertake other obligations set forth by the GDPR regarding such kind of transfer.

In particular, we may transfer your personal data to other companies in the Hisense group and our distributors that sell our products and services in certain markets or provide other services in relation to business support, complaints of ordered goods or customer support. A list of our companies in certain countries and their external contractors that may have access to the personal data of users from certain markets is listed in the Appendix link.

These external contractors help us to provide you with the requested services. While doing so, they act as data processors who process your personal data on our behalf. However, certain external contractors can have the role of data controller at the same time. This is because they can also process your personal data for purposes determined by themselves. For example, for improving and enhancing the quality of their business processes, for resolving any kind of technical issues they might have within their systems, etc. Since we do not control them when they process your personal data for their own purposes, it is important that you familiarize yourself with their own privacy policies linked below.
The Company may disclose your information if we believe that the disclosure is required by law, if we believe that the disclosure is necessary to enforce our agreements or policies, in response to valid requests by public authorities (e.g., a court or a government agency), or if we believe that the disclosure will help us investigate or prevent crimes (including fraud) or protect the rights, property, or safety of the Company or our customers. We may also share your information with our data protection officers, legal counsels and other professional advisors, for the management of our business and for legal compliance purposes.

We may transfer your personal data acquired based on your consent according to this data protection policy to advertising and social networks, in particular to:

- Google Ireland Limited (registered number: 368047), with registered office at Gordon House, Barrow Street, Dublin 4, Ireland; the company's privacy policy is available here: LINK
- Facebook Ireland Limited, with registered office at 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, D02 X525, Ireland; the company's privacy policy is available here: LINK
- Pinterest, Inc., with registered office at 505 Brannan Street San Francisco, CA 94107 United States, the company's privacy policy is available here: LINK
- LinkedIn as a tool provided by Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA, LinkedIn's privacy policy is available here: LINK

To process personal data, we also use the services of other external contractors. External contractors may include:

- cloud computing service providers and other technology support providers such as
    - Microsoft Azure, provided by Microsoft Corporation, One Microsoft Way, Redmond, Washington 98052, USA, the company's privacy policy is available here: LINK
    - SAP Hybris provided by SAP SE, Dietmar-Hopp-Allee 16, 69190 Walldorf/Germany, the company's privacy policy is available here: LINK
    - Salesforce Marketing Cloud and Salesforce Service Cloud provided by Salesfor ce, Inc. Salesforce Tower, 415 Mission Street, 3rd Floor, San Francisco, CA 94105, United States, the company's privacy policy is available here: LINK
    - Cloudera provided by Cloudera, Inc., 5470 Great America Parkway, Santa Clara, CA 95054, USA, the company's privacy policy is available here: LINK
    - Tuya IoT platform provided by Tuya Global Inc., 3979 Freedom Circle, Suite 340, Santa Clara, CA 95054, the company's privacy policy is available here: LINK
    - DigitalOcean, 101 6th Ave New York, NY 10013, the company's privacy policy is available here: LINK
    - Cloudflare France SAS, 6 place de la Madeleine, 75008 Paris, the company's privacy policy is available here: LINK
    - Amazon Web Services, Inc., 410 Terry Avenue North Seattle, WA 98109 United States, the company's privacy policy is available here: LINK

- marketing tools providers that help us optimize the web and personalize content and offers for you, such as:
    - AV STUDIO d.o.o., Koroška cesta 55, 3320 Velenje, the company's privacy policy is available here: LINK
    - Agilcon, d.o.o., Letališka cesta 32, 1000 Ljubljana, the company's privacy policy is available here: LINK
    - ZenLab d.o.o., Polule 77C, 3000 Celje, the company's privacy policy is available here: LINK

- Columbus Global Lautrupvang 6, Ballerup, Denmark 2750, the company's privacy policy is available here: LINK
- Sprinklr, Inc. 29 West 35th Street, New York, NY 10001, USA, the company's privacy policy is available here: LINK
- Freshworks Technologies B.V. Stationsplein 32, 3511 ED Utrecht, the company's privacy policy is available here: LINK
- "eXpoint" SIA, rīvības street 76-34, Riga, LV-1001, the company's privacy policy is available here: LINK
- Mailchimp as a tool provided by Intuit Inc., 2700 Coast Avenue, Mountain View, CA 94043, the company's privacy policy is available here: LINK
- 24TTL B.V., Amsterdam, Noord-Holland, The Netherlands, the company's privacy policy is available here: LINK
- eStoreMedia sp. z o.o., Aleja Komisji Edukacji Narodowej 18, 02-722 Warszawa, Poland, the company's privacy policy is available here: LINK
- SiteOne Landscape Supply, Inc, 300 Colonial Center Parkway Suite 600 Roswell, GA 30076 United States, the company's privacy policy is available here: LINK
- Campaign Monitor Holdings Pty Ltd, 5 STAPLETON AVE SUTHERLAND NSW C3 2232, the company's privacy policy is available here: LINK
- Splunk Inc., 270 BRANNAN STREET SAN FRANCISCO CA 94107, the company's privacy policy is available here: LINK
- Twilio Inc., 101 Spear Street, Ste 500, San Francisco, CA 94105, the company's privacy policy is available here: LINK

- call centres and providers of tools for managing and recording telephone calls, especially:

  - Hisense Europe Customer Care Centar, Strahinjića bana 9, 11000 Beograd, Serbia;
  - 3CX, 4010 Boy Scout Boulevard, Suite 325, 33607, Tampa, Florida, USA, the company's privacy policy is available here: LINK
  - Vonage Business Limited, Rosalind House, Jays Close Basingstoke Hampshire RG22 4BS United Kingdom, the company's privacy policy is available here: LINK
  - Cisco Systems, Inc., 170 West Tasman, Dr.San Jose, CA 95134 USA, the company's privacy policy is available here: LINK.

- external service providers for the maintenance and repair of our devices.

- processors of external communication, especially communication via SMS messages and chat rooms, especially:
  - LiveChat, Inc. (101 Arch Street, 8th Floor, Boston MA 02110, United States of America, the company's privacy policy is available here: LINK
  - Jivochat as a tool provided by Lucas Loureiro Carvalho Suporte Tecnico ME., the Rua Neves Armond, 140, Sala 301, Praia Do Suá. Vitória, ES/Brazil, the company's privacy policy is available here: LINK
  - TargetFirst, 23 rue de la Croix Lormel, 22190 PLERIN, the company's privacy policy is available here: LINK
  - Freeday BV, Reg. No. 80204589, Vijverhof 47, 3032SB, Rotterdam, Netherlands, the company's privacy policy is available here: LINK

- companies that prepare surveys for us regarding user satisfaction with our products and services, especially:
  - Trustpilot A/S, Pilestraede 58, 5th floor, DK-1112 Copenhagen K, the company's privacy policy is available here: LINK.
  - Bazaarvoice, Inc., 10901 Stonelake Blvd, Austin, TX 78759, the company's privacy policy is available here: LINK
  - Reevoo, 2nd Floor Walbrook Wharf, 78-83 Upper Thames Street, London EC4R 3TD, the company's privacy policy is available here: LINK
  - Momentive Europe UC, 2 Shelbourne Buildings, Second Floor, Shelbourne Rd Ballsbridge, Dublin 4, Ireland, the company's privacy policy is available here: LINK

From time to time, the company organizes prize games and similar promotional campaigns together with third parties, to whom it may also provide individual personal data, whereby you will be informed of this prior to the collection of personal data.

11. Where do we store your data?

Your data are stored within company internal server units and workstations (also using cloud technologies) and in the data lake system (a data lake is a centralized repository that allows you to store structured and unstructured data at any scale).

12. Notice to residents of certain states in the United States

This supplemental notice to the Data Protection Policy is intended for residents of the United States who reside in states that have a comprehensive consumer privacy law currently in effect. This supplemental notice describes how residents of such states, including California, Colorado, Connecticut, Oregon, Texas, Utah and Virginia, may exercise rights under the consumer privacy laws applicable to their state of residence ("U.S. State Privacy Laws").

The definition of "personal information" depends on the applicable law in your U.S. State Privacy Law state. For purposes of this supplemental notice, "personal information" is any data that identifies or makes an individual identifiable. Personal information does not include information that is publicly available, deidentified or aggregated, or otherwise excluded from the scope of applicable U.S. State Privacy Laws.

Consumer Privacy Rights

Depending on the applicable law where you reside, you may be able to assert certain rights identified below with respect to your personal information. If any of the rights listed below are not provided to you under the law that governs the processing of your personal information, we have full discretion in providing you with those rights. Please refer to the table below to determine the rights you have in your jurisdiction.

Your rights in relation to your personal information are not absolute. Depending upon the applicable law, access to your rights under the applicable law may be denied: (a) when denial of access is required or authorized by law; (b) when granting access would have a negative impact on another's privacy; (c) to protect our rights and properties; or (d) where the request is frivolous or vexatious, or for other reasons.

Privacy rights include the following:

a. **Right to Know/Access.** You may have the right to obtain a copy, or a list of categories of the personal information that we hold about you, as well as other supplementary information, such as the purposes of processing, and the entities to whom we disclose your personal information.

b. **Right to Correct.** You may have the right to correct any of your personal information in our records and systems that is inaccurate.

c. **Right to Delete.** Under certain circumstances, you may have the right to request that we delete the personal information that we hold about you. This right is not absolute, and we may refuse such a request if there are compelling legitimate grounds for keeping your personal information or as required by law. In addition, in the event your deletion request is honored, we may retain a record of your deletion request as required under applicable laws and their exceptions.

d. **Right to Portability.** You may have the right to receive a copy of the personal information we have collected about you in a structured, commonly used and machine-readable format.

e. **Right to Opt-Out Sale / Right to Opt-Out of Sharing for Targeted Advertising.** You may have the right to opt-out of: (i) the sale of your personal information to third parties; and (ii) the sharing of your personal information for targeted advertising. While we do not sell your personal information for money, we use cookies, pixels, software development kits, advanced programming interfaces, third-party integrations within our device operating systems, and similar technology, and we make available certain information, such as your IP address or device identifiers, to certain third-party advertising partners in order to improve your user experience and to optimize our marketing activities. Under some state privacy laws' broad definition of "sell", this could be considered a sale, and it could be considered "sharing" of your personal information for targeted, cross-context behavioral advertising purposes.

You have the right to direct us not to sell your personal information to third parties, and to direct us not to share or use your personal information for targeted advertising purposes. To exercise your right to opt-out, please submit a request by mail to privacy@connectlife.io. Please note that you may still receive generalized ads after opting out of targeted advertising.

f. **Right to Limit Use and Disclosure of Sensitive Personal Information.** If you are a California resident, to the extent your sensitive personal information, as that term is defined under California privacy law, is used to infer characteristics about you, you have the right to object to our processing of your sensitive personal information. We do not use sensitive personal information to infer characteristics about you.

g. **Right to Opt-Out of Automated Decision-making or Profiling.** You may have the right not to be subject to a decision which significantly impacts your

rights that is based solely on automated processing (where a decision is taken about you using an electronic system without human involvement). No decision will be made by us about you solely on the basis of automated decision making which has a significant impact on you.

h. **Right Against Discrimination.** You may have the right not to be discriminated against for exercising any of the rights described in this section. We will not discriminate against you for exercising your rights.

i. **Right to Appeal.** In certain jurisdictions, you may have the right to appeal if we refuse to take action on your rights request. Instructions on how to appeal will be provided to you upon such a denial, but in any event, such instructions will be substantially similar to those provided below for submitting requests.

j. **Shine the Light.** If you are a California resident, you have the right to ask us for a notice describing what categories of personal information we share with third parties or corporate affiliates for those third parties' or corporate affiliates' direct marketing purposes.

k. **Right to Withdraw Consent.** In certain jurisdictions, to the extent the processing of your information is based on your consent, you may withdraw your consent at any time. Your withdrawal will not affect the lawfulness of our processing before your withdrawal.

l. **Marketing Communications.** You may choose to provide us with your email address to send free newsletters, surveys, offers, and other promotional materials to you, as well as targeted offers from third parties. You can stop receiving promotional emails by following the unsubscribe instructions in emails that you receive. If you decide not to receive promotional emails, we may still send you service-related communications."

Please note that "unsubscribe" requests may not take effect immediately and may take a reasonable amount of time to receive, process, and apply, during which time your information shall remain subject to this Data Protection Policy. Additionally, you should be aware that any information provided to third-parties prior to your election to unsubscribe will not be retrieved or rescinded, unless required by applicable law.

As mentioned above, depending on where you reside, you may be able to assert certain rights with respect to your personal information. To determine which rights you have, please refer to the table below that references the rights as described above in the "Consumer Privacy Rights" section. Any places that are not listed either do not have a law providing such rights, or their law does not apply to our operations.

California Residents: (a) Right to Know/Access; (b) Right to Correct; (c) Right to Delete; (d) Right to Portability; (e) Right to Opt-Out of Sale / Right to Opt-Out of Sharing for Targeted Advertising; (f) Right to Limit Use and Disclosure of Sensitive Personal Information; (g) Right to Opt-Out of Automated Decision-making or Profiling (upon issuance of regulations by the California Privacy Protection Agency); (h) Right Against Discrimination; and (j) Shine the Light.

Colorado, Connecticut, Virginia, Oregon, Texas, Utah Residents: (a) Right to Know/Access; (b) Right to Correct; (c) Right to Delete; (d) Right to Portability; (e) Right to Opt-Out of Sale / Right to Opt-out of Sharing for Targeted Advertising; (g) Right to Opt-Out of Automated Decision-making or Profiling; (h) Right Against Discrimination; (i) Right to Appeal; and (k) Right to Withdraw Consent.

Residents of other States, including those listed above: (a) Marketing Communications; and (b) Right to Correct

Submitting a Request to Exercise Your Rights. In addition to the methods specified above, you may exercise these rights by submitting a request by mail to privacy@connectlife.io.

Before fulfilling your request, we may be required by law to have you to verify the personal information we already have on file to confirm your identity. If we cannot verify your identity based on the information we have on file, we may request additional information from you, which we will only use to verify your identity, and for security or fraud-prevention purposes.

Special Notice to California Residents

This section applies solely to individuals who reside in the State of California. The purpose of this section is to inform California residents ("consumers" or "you"), at or before the time of collection of personal information, about our data collection practices and your privacy-related rights under California law, including the California Consumer Privacy Act of 2018, as amended ("CCPA").

In the preceding twelve months we may have disclosed these categories of personal information for a business purpose:

- Identifiers
- Personal information categories listed in the CCPA
- Commercial information
- Internet or similar network activity
- Inferences drawn

The sources of this personal information, the purposes of information collection and the sharing of this personal information are outlined within this Data Protection Policy.

13.Notice to residents of Canada

a. Consent. We will obtain your consent to collect, use or disclose personal data except where we are authorized or required by law to do so without consent. For example, we may collect, use or disclose personal data without your knowledge or consent where: the information is publicly available, as defined by statute or regulation; we are obtaining legal advice; or we reasonably expect that obtaining consent would compromise an investigation or proceeding. Other exceptions may apply. Your consent can be express, implied or given through an authorized representative. Consent may be provided orally, in writing, electronically, through inaction (such as when you do not notify us that you

do not wish your personal data collected/used/disclosed for various purposes after you have received notice of those purposes) or otherwise.
You may withdraw consent at any time, subject to legal, contractual and other restrictions, provided that you give us reasonable notice of your withdrawal of consent. If you notify us that you withdraw consent, we will inform you of the likely consequences of that withdrawal, which may include our inability to provide certain services for which that information is necessary.

b. Limits on Collection of Personal Data. We will not collect personal data indiscriminately but will limit collection of personal data to that which is reasonable and necessary. We will also collect personal data as authorized by law.

c. Limits for Using, Disclosing, and Retaining Personal Data. Your personal data will only be used or disclosed for the purposes set out above and as authorized by law. We will keep your personal data for as long as necessary in connection with the purposes identified above or as permitted or required by law. You must notify us if you no longer want us to retain your information.

d. Location of Service Providers, Hosting and Servers. Our service providers may be located outside of the country in which you are located, and our servers are currently located in the European Union. You therefore acknowledge that your personal data may be processed and stored in foreign jurisdictions and that governments, courts, law enforcement or government or regulatory agencies in the EU and elsewhere may be able to access or obtain disclosure of your personal data under a lawful order or otherwise through the laws of the applicable jurisdiction, irrespective of the safeguards we have put in place for the protection of your personal data.

e. Access to my Personal Data. You may modify personal data that you have submitted by logging into your account and updating your profile information. Please note that copies of information that you have updated, modified or deleted may remain viewable in cached and archived pages of the Site or Application for a period of time.
In some situations, we may not be able to provide access to certain personal data. This may be the case where, for example, disclosure would reveal personal information about another individual, the personal information is protected by solicitor/client privilege, the information was collected for the purpose of an investigation or where disclosure of the information would reveal confidential commercial information that, if disclosed, could harm our competitive position. We may also be prevented by law from providing access to certain personal data. When an access request is refused, we will notify you in writing, document the reasons for refusal and outline further steps which are available to you.

f. Amendment to my Personal Data. If you demonstrate the inaccuracy or incompleteness of personal data, we will amend the information as required. Requests to modify any information you have provided us may be submitted to privacy@connectlife.io. Please allow up to thirty (30) days for us to process and respond to your request.

g. Limitations on Deletion of Data. You may request deletion of your personal data by us, however, we may be required (by law or otherwise) to keep this information and not delete or anonymize it. When we delete or anonymize personal data, it will be deleted from the Services' active database, but your personal data may remain in our archives.

If we disclose some of your personal data to third parties, we may no longer have access to that personal data and cannot force the deletion or modification of any such information by those third parties. After we delete or anonymize personal data, we may retain de-identified information, and will continue to use the information as permitted under this Data Protection Policy.

i. What choices do I have regarding use of my Personal Data? We may send periodic promotional emails to you. You may opt-out of promotional emails by following the opt-out instructions contained in the email. Please note that it may take up to 10 business days for us to process opt-out requests. If you opt-out of receiving promotional emails, we may still send you emails about your account or any services you have requested or received from us. You may also withdraw your consent to our collections, uses and disclosures of your information at any time, subject to legal, contractual and other restrictions and technical limitations, provided that you give reasonable notice of withdrawal of consent to us. On receipt of notice of withdrawal of consent, we will inform you of the likely consequences of the withdrawal of consent, which may include our inability to provide certain services for which that information is necessary.

14. Notice to residents of Mexico

You have the right to (i) access your personal data; (ii) rectify your personal data, if they are inaccurate or incomplete; (iii) cancel your personal data; and (iv) oppose the use of your personal data for specific purposes (jointly, the "**ARCO Rights**"). In case you wish to exercise any of the ARCO Rights, please send an email to the account privacy@connectlife.io, which must contain, at least, the following information:

- Full name and email address or address, in order to communicate the response to your request.
- The documents that prove your identity, or if applicable, that of your legal representative.
- A clear description of the personal data with respect to which you seek to exercise any of the ARCO Rights.
- Any other element or document that facilitates the location of personal data.

If required, we may request additional information. The response to your request will be communicated to you within the following 15 (fifteen) business days and, if it is appropriate, it will be implemented within a maximum period of 20 (twenty) business days.

a. How can you revoke your consent to the use of your Personal Data? You can revoke the consent that, in your case, you have given us for the processing of your personal data. However, it is important that you bear in mind that not in all cases we will be able to respond to your request or terminate the use immediately, since it is possible that due to some legal obligation, we will need to continue processing your personal data. Likewise, you should consider that for certain purposes, the revocation of your consent will imply that we cannot continue to provide the service you requested, or the conclusion of your relationship with us. To revoke your consent, or to inquire as to the procedure and requirements for doing so, you must submit your request at privacy@connectlife.io.

b. How can you limit the use or disclosure of your Personal Data? In order for you to limit the use and disclosure of your personal data, we offer you the following means:

Your registration in the Public Registry to Avoid Advertising (*Registro Público para Evitar Publicidad*), which is in charge of the Federal Consumer Prosecutor's Office (*Procuraduría Federal del Consumidor*), so that your personal data is not used to receive advertising or promotions from goods or services companies. For more information about this registry, you can consult the PROFECO Internet portal, or you can contact it directly.

Your registration in our exclusion list, so that your personal data is not processed for marketing, advertising or commercial prospecting purposes by us. For more information, you can contact us at privacy@connectlife.io.

Non-conformity or complaint to the INAI

If you consider that your right to the protection of personal data has been damaged by any conduct or omission on the part of the Company, or you presume any violation of the provisions set forth in the Law, its Regulations and other applicable regulations, you may file your disagreement or complaint before the National Institute of Transparency, Access to Information and Protection of Personal Data (INAI). For more information, we suggest you visit their official website: www.inai.org.mx.

15. Do not track settings

Certain country/state/province laws require that we indicate whether we honor "Do Not Track" settings in your browser concerning targeted advertising. We adhere to the standards set out in this Data Protection Policy and do not monitor or follow any Do Not Track browser requests.

16. What are your rights and how to exercise them

You can exercise the following rights regarding your personal data we process:

- Right of access – enables you to obtain the information as to whether your personal data is being processed and regarding the procedures and methods of personal data processing,
- Right to rectification – in case you notice that your data is not accurate, you have the right to complete incomplete or to correct the incorrect data,
- Right to erasure – allows you to request the erasure of your personal data that we process. We will do this in accordance with the GDPR and in the event that there are no other restrictions preventing us from doing so,
- Right to restrict processing - allows you to restrict processing, while you dispute the accuracy of the data, object to deletion, as the purpose of the processing for which the data was collected is no longer relevant, and you want further storage due to legitimate interests, or if you have submitted a request to determine the legal reasons for processing,
- Right to data portability – allows you to receive a copy of the provided personal data in a structured, commonly used hardware format, and to transmit data to another controller, if the requirements set forth by the GDPR are met,

- Right to object - enables objection in case of data collection and processing for the purposes of direct marketing or related profiling,
- Right to review automated decision-making - in the event that a decision that is reflected in our mutual relationship is based on automated decision-making, you can use the right to implement a new, non-automated decision,
- Right to withdraw consent – in the event that the processing is based on the given consent, you have the right to revoke the consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal.

If you wish to use any of the above rights, you can do so by notifying us at the e-mail address privacy@connectlife.io.

In addition to the above rights, you also have the right to lodge the complaint with the supervisory authority. In the event that your rights regarding the processing of personal data have been violated, you can file a complaint with the competent authority:

- For company ConnectLife, data technologies, LLC: Information Commissioner of the Republic of Slovenia, by mail to the address: Dunajska 22, 1000 Ljubljana or via e -mail to the address: gp.ip@ip-rs.si
- For Hisense UK ltd: Information Comissioner of the United Kingdom by mail to: Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF, or view email to: icocasework@ico.org.uk

17. Data Protection Officer

In all matters related to the processing of your personal data, our data protection officer is at your disposal and can be contacted at the e-mail address: privacy@connectlife.io.

18. Compliance with the EU Data Act

In accordance with the requirements set out in the EU Data Act (Regulation (EU) 2023/2854), we are committed to providing access to data, including metadata (e.g., information on the usage of appliances or connected devices), to you as a user and third parties where such access is required under the EU Data Act and all conditions established by the EU Data Act are fully satisfied. Detailed pre-contractual information regarding the non-personal data collected upon usage of the device when connected in the ConnectLife mobile app is provided in the EU Data Act User Data Notification, available here: EU Data Act User Data Notification V2.0 - ConnectLife.

We stress that the application of the EU Data Act does not override, limit, or abolish any obligations under the GDPR, including but not limited to data minimization, purpose limitation, data subject rights, and security of processing. We remain fully compliant with all applicable provisions of the GDPR in parallel with our obligations under the EU Data Act.

19. Data Protection Policy Versions and Changes

We reserve the right to change this Data Protection Policy at any time or for any reason. If we make any material changes, we will post the updated Data Protection Policy in the

same way as this version with a “Last Updated” effective date of the revisions. This Data Protection Policy will remain in full force and effect as long as you are a user of our appliances, services and websites, even if your use of or participation in any particular service, feature, function or promotional activity terminates, expires, ceases, is suspended or deactivated for any reason. We encourage you to look for updates and changes to this Data Protection Policy when using our appliances, accessing our websites and our services. If you have any questions about this Data Protection Policy, please reach out anytime as described in the previous section above.