

Privacy Statement

Effective Date: May 1, 2025

HM Electronics, Inc. and each of its affiliates (collectively, "HME", "we", "us" or "our") respect your privacy and are committed to processing your personal data in accordance with the law.

This Privacy Statement (hereinafter the "Statement" or "Privacy Statement") applies to all applications, websites and domains owned by HME linking to or posting this Statement, including www.hme.com; www.hme.com/qsr; www.clearcom.com; www.clearcom50.com; www.trilogycomms.com; www.cerepairs.com; www.hmedtcloud.com; customerservice.hme.com; customerservice.cerepairs.com; and customerservice.clearcom.com ("Website" or "Websites").

This Privacy Statement describes how we collect, use, store, disclose and process personal data that we obtain through or in connection with the use of our Websites, including through or in connection with purchases of our products and services, through or in connection with use of the HME Careers Portal, the Customer Portal, the HME Cloud, our drive-thru products and services including the Zoom® and Nexeo® drive-thru systems, the Clear-Com Partner/Consultant Portal and SkyPort™, the Clear-Com Agent-IC® and Station-IC™ applications and Gen-IC™, or when you otherwise contact us and/or we collect your personal data.

HME reserves the right to change, modify and update this Privacy Statement from time to time by posting a revised version on our Websites, and by revising the "Effective Date" at the top of this Statement. If considered necessary, we will also notify you directly of any change.

Therefore, we recommend you regularly consult this Statement to make sure that you are aware of any changes.

We do not knowingly collect or store any personal data from anyone under the age of 18. If we become aware that we have collected or stored personal data from an individual under age 18, we will remove their personal data from our files. If you are a parent or guardian and believe we may have inadvertently collected personal data from your child, please notify us via email to privacy@hme.com.

1. General

- 1.1. The term "personal data" as used in this Statement shall mean any information (including "personal information" as that term may be defined in applicable privacy law) that actually enables, or is capable of enabling us to identify you, directly or indirectly, by reference to an identifier such as your name, identification number, location data, online identifier or one or more factors specific to you.
- 1.2. For the purposes of the General Data Protection Regulation 2016/679 (the "GDPR") and other laws globally, the HME entity that is responsible for your personal data ("data controller") is the HME entity from which you have purchased products and/or services, or with which you have applied for a job or entered into communications, or which has otherwise collected your personal data. For further details on each HME data controller, please see below.
- 1.3. If you have questions about this Privacy Statement or the manner in which HME collects, uses or otherwise processes your personal data, please contact the Privacy Team at the relevant HME data controller using the contact details below:

HM Electronics, Inc.

By post: 2848 Whiptail Loop, Carlsbad, CA 92010, USA

By email: privacy@hme.com

Clear-Com LLC ("Clear-Com")

By post: 1301 Marina Village Parkway, Suite 105, Alameda, CA 94501, USA

By email: marketing@clearcom.com

Clear-Com Research Inc.

By post: Data Protection Officer, 1430 Hocquart, Suite 101 St-Bruno-de-Montarville, Quebec J3V 6E1 Canada

By email: marketing@clearcom.com

With a copy to the Data Protection Officer: Marco Lopez privacy@clearcom.com

Trilogy Communications Limited

By post: 2000 Beach Drive, Cambridge Research Park, Cambridge CB25 9TP, United Kingdom

Online at: trilogycomms.com/en/contact

Commercial Electronics, Inc.

By post: 3787 Rider Trail S., Earth City, MO 63045, USA

By email: Privacy@ceinstl.com

- 1.4. The Websites may, from time to time, contain links to and from the websites of our partner networks, advertisers, and other third parties. If you follow a link to any of these websites, please note that these websites may have their own privacy statements and that we do not accept any responsibility or liability for these statements. Please check these statements before you submit any personal data to these websites.

2. Careers with HME

- 2.1. HME's Careers Portal (accessible by following the 'careers' link on our applicable Websites) allows you to apply for positions with HME. Moreover, it offers you the opportunity, without application to a particular position, to submit the information that will allow HME to contact you if suitable openings arise in the future (provided you have given your consent to be contacted in such an event).
- 2.2. Registering for the Careers Portal requires you to submit specific personal data. You are under an obligation to provide only personal data which is accurate, complete and up to date at the time at which you submit it to the Careers Portal.
- 2.3. The open career opportunities published on our Websites do not constitute an offer or promise of employment and HME may eliminate, modify or change without notice any aspect(s) of the employment positions, compensation, and benefit plans described therein. Our Websites provide descriptions of possible positions within HME, and do not provide binding offers nor terms and conditions of employment. Any employment offer that may follow as a result of the identification of a potential opportunity by an applicant or submission of information to HME is in accordance

with the specific terms of that offer.

- 2.4. Please note, by entering your eSignature and clicking "submit", you acknowledge and agree that your personal data will be processed in order to process your employment application in accordance with this Statement. If your application is unsuccessful, we will store your personal data for up to six (6) months (or such longer period as may be required by applicable law) in the Careers Portal following the conclusion of the unsuccessful application, in order to respond to any questions you might have about your application and in order to protect ourselves from legal claims. With your consent, we may retain your personal data for the purposes of identifying and contacting you about other suitable recruitment opportunities within HME globally for a further five (5) year period, unless you withdraw your consent or deactivate your profile, which you may do at any time. Deactivating your profile will withdraw all your applications from all the positions you have applied to within HME and will remove your profile from the Careers Portal. However, if you have applied for a position within HME, your personal data may be retained for a temporary period of time in an "inactive" status as required by applicable law and may not be deleted immediately. While you may request that we delete your personal data, we will not be able to process your job application as a result.

3. Categories of Personal Data HME Collects

- 3.1. We may collect and process the following categories of personal data:

3.1.1. Personal data provided to us.

Suppliers, vendors, customers, authorized users of our products and/or services, partners and Website visitors provide personal data to us in many ways, for example by filling in online feedback and contact forms, requesting information, purchasing HME products, subscribing to materials and newsletters, participating in surveys, signing up for the Customer Portal and providing information during the recruitment process, the HME Cloud, our drive-thru products and services including the Zoom® and Nexeo® drive-thru systems, the Clear-Com Partner/Consultant Portal and SkyPort™, the Clear-Com Agent-IC® and Station-IC™ applications and Gen-IC™. This includes personal data, such as:

- a) **Identifiers**, including name, title, alias, date of birth, marital status, postal address, email address, phone number, passport number, unique personal identifiers (such as log-in details, your username and password and customer ID) and the company you represent;
- b) **Commercial information**, such as transaction history, products/services purchased, obtained or considered etc.; and
- c) **Financial and transaction data**, including bank account and payment card details and information about payments from you and other details of products and services you have purchased from us.
- d) **Sensitive Personal Information**, such as Social Security or other tax identification number, financial account, debit card, or credit card number in combination with any required security or access code, or precise geolocation.

If you sign up for the Careers Portal and apply for work with us, or if you are a current or former employee, we may collect, store, and use the following categories of personal data that you have provided to us in your curriculum vitae, a covering letter, on an application form or during an interview or onboarding, or that we have received from a recruitment agency, reference, or

background check provider:

- a) **Identifiers**, including name, title, alias, date of birth, marital status, postal address, email address, phone number, passport number, unique personal identifier, Social Security or other tax identification number, preferred job role and HME office location;
- b) **Protected Information** such as name with: Social security or other tax identification number, driver's license or state ID number, financial account, medical, health, and health insurance information, user name and password;
- c) **Protected anti-discrimination classification information**, such as age (40 years or older), race, national origin, citizenship, marital status, medical condition, physical or mental disability, sex (including gender, gender identity, pregnancy or childbirth and related medical conditions), and veteran or military status;
- d) **Professional or employment-related information**, such as employment history, qualifications, answers to questions about suitability for a position, preferred job conditions, extracurricular activities, professional references and professional and personal competencies;
- e) **Education information**, such as academic qualifications and education records;
- f) **Electronic network activity**, such as your use of HME systems, browsing or search history, or website interactions; and
- g) **Sensitive Personal Information**, such as Social Security or other tax identification number, driver's license, passport number or other government-issued identification information, account log-in, financial account, debit card, or credit card number in combination with any required security or access code, password, or credentials allowing access to an account, precise geolocation, and consumer's racial or ethnic origin.

3.1.2. **Personal data we collect via our Websites.**

We also collect the following information indirectly from you when you access our Websites, use our interactive chat function, or otherwise correspond with us via our Websites:

- a) **Identifiers**, such as the phone number or email address used to correspond with us;
- b) **Audio, video or similar information**, such as call center phone call recordings and security camera video recordings at our facilities;
- c) **Internet or other similar network activity**, such as limited technical information including information on your IP address, browsing or search history, website interactions, advertisement interactions, browser type and version, time zone setting and location, operating system and platform, page interaction information, and the type of device used to access our Websites; and
- d) **Geolocation**, limited to town or city level information based on your IP address.

We may collect such internet or other similar network activity data using cookies and similar technologies. For more information about our practices in this area for a particular Website, please see our Cookie Notice linked in the footer of such Website.

3.1.3. **Personal data we collect via our products and services.**

We collect personal data through the use of our products and services, which may include:

- a) **Clear-Com Agent-IC®, Station-IC™ and Gen-IC™ Applications:** These applications may access and transmit audio data from your device to Clear-Com systems and third-party equipment connected to the applicable audio ports. The audio data is encrypted using AES-128 technology for security. The applications also collect and store user profiles (including network addresses, usernames, and passwords) locally on the device or in Clear-Com's cloud services. The applications automatically check for updates, collect technical data such as usage, device type, application version, and platform performance metrics, and may gather data for technical support purposes. Users may opt to share such data with us when requesting support.
- b) **Drive-thru Products and Services (Zoom®, Nexeo®, etc.):** Our drive-thru systems may collect and process personal data, including identifiers for authorized users (e.g., name, email) and voice recordings, to provide dashboards, quality control and training analytics. The systems also collect technical data, including performance data related to service times (e.g., data relating to the time it takes to fulfil drive-thru orders). This data is used to deliver various features such as enabling staff to send voice notes, voice-activated services (such as automated order taking systems), order tracking, curbside services, and performance analytics. Data collected may be hosted on HME Cloud servers located in the United States. Our customers are responsible for ensuring that their use of these products and services, and their collection and processing of personal data, complies with all applicable privacy laws.
- c) **HME Cloud and Other Cloud Services:** We host data relating to drive-thru system performance and authorized users in the HME Cloud, which may include personal data like identifiers (name, email). By accessing these services, particularly from outside the United States, you consent to the storage and processing of your data in the U.S.
- d) **Technical and Performance Data:** Across our products and services, we may collect technical data on application performance, system usage, device type, and aggregated metrics to improve our services. This data does not directly identify individuals but may be used to optimize user engagement and service offerings.

4. **How HME uses personal data**

- 4.1. We will only process your personal data in accordance with this Statement and the applicable law. Where applicable law requires us to have a legal basis for processing your personal data, we rely on one or more of the following legal bases:
 - 4.1.1. **Performance of a contract with you:** Where we need to process personal data for the performance of a contract between you and us or to answer questions or take steps at your request prior to entering into a contract.
 - 4.1.2. **Legitimate interests:** We may use your personal data where it is necessary to conduct our business and pursue our legitimate interests.
 - 4.1.3. **Legal obligation:** We may use your personal data where it is necessary for compliance with a legal obligation that we are subject to.

4.1.4. **Consent:** We rely on consent only where we have obtained your active agreement to use your personal data for a specified purpose, for example if you subscribe to an email newsletter.

4.2. We have set out below, in a table format, a description of all the ways we plan to use the various categories of your personal data relating to suppliers, vendors, customers, authorized user of our products and/or services, partners or Website visitors, and which of the legal bases we rely on to do so.

Purpose	Type of data	Legal basis
To administer and fulfil our obligations under any agreements to which we are a party, including allowing purchases, tracking shipments, and processing invoices.	Identifiers; Commercial information; Financial and transaction data; Sensitive personal information.	(a) Performance of a contract (b) Our legitimate interests (to provide our products/services)
To manage and respond to your interactions with us, including handling queries, requests, and providing technical, sales, and after-sales support.	Identifiers; Commercial information.	(a) Performance of a contract (b) Our legitimate interests (to provide effective customer service and to keep our records updated and manage our relationship with you and to keep our records updated)
To create, manage, and allow access to your customer account, including enabling you to log in, configure settings, manage restaurant layouts, upgrade plans, and change preferences.	Identifiers; Commercial information.	(a) Performance of a contract (b) Our legitimate interests (to provide effective customer service and to keep our records updated and manage our relationship with you and to keep our records updated)
To notify you of updates to our services, including changes to our terms or policies, and to provide relevant information about your account.	Identifiers; Commercial information.	(a) Performance of a contract (b) Our legitimate interests (to provide our products/services and to keep our records updated)
To administer promotions, competitions, and surveys, allowing participation and offering personalized promotional benefits.	Identifiers; Commercial information.	(a) Our legitimate interests (to study how customers use our products/services, to develop them and grow our business) (b) Your consent (where required by law)
To ensure compliance with applicable laws and regulations, including responding to legal requests or regulatory inquiries.	Identifiers; Commercial information; Financial and transaction data;	(a) Our legitimate interests (to protect our legal rights and ensure compliance with applicable laws)

	Sensitive personal information.	(b) To comply with our legal obligations
To protect, enforce, or defend our rights and resolve any disputes, including monitoring quality control and ensuring compliance.	Identifiers; Commercial information; Financial and transaction data; Sensitive personal information.	(a) Our legitimate interests (to protect our legal rights and ensure compliance with applicable laws) (b) To comply with our legal obligations
To ensure the security of our systems and your account, preventing and detecting fraud or malicious activity, and maintaining the safety and security of our websites and computer systems.	Identifiers; Commercial information; Internet or other similar network activity.	(a) Our legitimate interests (to protect our business and network security and to prevent fraud) (b) To comply with our legal obligations
To administer and improve our internal operations and business administration, including troubleshooting, data analysis, testing, research, and statistical and survey purposes.	Identifiers; Commercial information; Internet or other similar network activity.	(a) Our legitimate interests (to improve business efficiency and performance)
To develop and enhance our products and services, including reviewing feedback, usage patterns, and customer preferences to meet your needs.	Identifiers; Commercial information; Internet or other similar network activity.	(a) Our legitimate interests (to improve and develop our services)
To personalize your experience and offer tailored services, including providing suggestions based on your previous requests and sending personalized marketing communications about products or services that may be of interest to you.	Identifiers; Commercial information; Internet or other similar network activity.	(a) Our legitimate interests (to provide personalized services) (b) Your consent (where required by law)
To measure and analyze the effectiveness of marketing initiatives and online advertisements, including using data analytics to improve our website, services, and customer experiences.	Identifiers; Commercial information; Internet or other similar network activity.	(a) Our legitimate interests (to understand the effectiveness of our marketing efforts) (b) Your consent (where required by law)

- 4.3. We have set out below, in a table format, a description of all the ways we may use the various categories of your personal data relating to job applicants, current and former employees, and which of the legal bases we rely on to do so.

Purpose	Type of data	Legal basis
To facilitate and manage your profile registration on the Careers Portal and to contact you regarding job applications, including corresponding if your profile and preferences match a vacant position, as long as your profile is active on the Careers Portal.	Identifiers; Professional or employment-related information; Education information	(a) Performance of a contract (b) Our legitimate interests (to manage the recruitment process and communicate with candidates about job opportunities)
To assess your qualifications with respect to your application for available positions within HME, including reviewing references, facilitating background screening, and deciding whether to enter into an employment relationship with you.	Identifiers; Protected information; Professional or employment-related information; Education information; Sensitive Personal Information	(a) Performance of a contract (b) Our legitimate interests (to assess your application and qualifications for a job position) (c) Necessary to comply with legal obligations (e.g., background checks, where required)
To transfer candidate data from the Careers Portal to our internal HR systems in the event of a successful application, to facilitate onboarding and manage your employment relationship with us.	Identifiers; Protected information; Protected anti-discrimination classification information; Professional or employment-related information; Education information; Sensitive Personal Information.	(a) Performance of a contract (b) Our legitimate interests (to manage your employment relationship and onboard new employees) (c) Necessary to comply with legal obligations
To comply with applicable laws, including antidiscrimination laws and disability accommodation laws, by processing protected antidiscrimination information and sensitive personal information.	Identifiers; Protected information; Protected anti-discrimination classification information; Professional or employment-related information; Education information; Sensitive Personal Information.	(a) Necessary to comply with legal obligations (e.g., anti-discrimination laws and disability accommodation requirements)

- 4.4. We may process your personal data in order to protect your vital interests or the vital interests of another person, for example in order to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety.
- 4.5. Notwithstanding any legal basis for processing personal data identified above, where required by applicable law, we will obtain consent for the processing of personal data, which consent may be express or implied depending on the circumstances.
- 4.6. In many instances, HME acts as a processor or a service provider on behalf of its customers. This

means that any personal data provided to us in connection with the use of our products/services will be processed in accordance with our customers' instructions, as necessary to provide and support the products and services. We do not access or use this personal data for any purpose other than to fulfill our contractual obligations to our customers, such as providing maintenance services, troubleshooting, or otherwise ensuring the proper functioning of our systems. The scope of processing is limited to what is required to deliver the agreed-upon products/services.

5. How long HME retains personal data

- 5.1. We will store your personal data, in a form that permits us to identify you, only as long as necessary for the purpose it was collected. The retention period is determined based on factors such as the duration needed to provide our services and operate our business, any applicable legal or contractual obligations, specific legal retention requirements, the sensitivity of the data, any consent for longer retention, and the expectations at the time the data was provided. We may also retain your personal data as necessary to comply with legal obligations, resolve disputes, and enforce our agreements and rights, or if it is not technically and reasonably feasible to remove it. Otherwise, we will seek to delete your personal data within a reasonable timeframe upon request.
- 5.2. If you choose a direct payment gateway to complete a purchase on the Websites, then PayPal Gateway stores your credit card data. Your purchase transaction data is stored in accordance with PayPal's retention practices.

6. Where HME stores personal data

- 6.1. We are headquartered in the United States. Your personal data will be stored on servers and will be accessed by us (including our authorized personnel) or transferred to us in the United States or to our affiliates, partners, or service providers who are located worldwide. By visiting our Websites from outside the United States, you acknowledge that your information may be transferred to, stored, and processed in the United States where our servers are located, and our central database is operated, as well as other countries where our service providers, partners or affiliates are located.
- 6.2. Where personal data is transferred from the European Economic Area, Switzerland or the United Kingdom to a country that has not received an adequacy decision by the European Commission or UK Secretary of State, we rely on appropriate safeguards. These include the European Commission-approved Standard Contractual Clauses (SCCs), the UK International Data Transfer Agreement (IDTA), or the ICO Addendum to the SCCs, as well as any supplementary measures that may be necessary, to transfer the data in compliance with applicable law.

7. How HME shares personal data

- 7.1. We will not sell, hire out, disclose, transfer or pass on your personal data to third parties, except in the situations provided for in this Statement or unless you provide prior consent. We may share personal data in the following ways:
 - 7.1.1. **Our Affiliates.** Your personal data may be accessed by us or transferred to us in the US and shared with our affiliates in order to process your personal data (the information shared includes identifiers, commercial information, financial and transaction data, internet or other similar network activity, professional or employment-related information and non-public education information). Such information may be shared so that affiliates can provide and share services relating to (amongst other things) HR, finance, customer care, quality review and management of vendors, distributors,

partners, suppliers, contractors and others, compliance with regulatory bodies and public authorities, supply chain and sourcing management, tendering, quoting and bidding for any private, public or governmental projects, and implementing and sharing information on the same, sales administration, technology services including research and development, business development, marketing activities and preparing business plans, IT, risk management, database management and analysis of commercial activities, administrative services, accounts and records, tax planning and compliance services, and marketing services.

- 7.1.2. **Third-party service providers.** We may share personal data with service providers and suppliers retained to deliver complete products, services and customer solutions and to assist us with marketing and communication initiatives, and service providers retained to assist us with staffing and employee administration. These service providers and suppliers include, for example, providers of site and store hosting services, providers of voice activated input/output software and related technology for automated order taking systems, customer support and live-help, IT and network vendors, marketing, email service providers, automated data processors, providers of payment processing and payroll services, employee benefits providers, and shipping agents. When we share your personal data with third parties that we engage to process data on our behalf, including our affiliates, we will ensure that those third parties are contractually bound to guarantee the same levels of privacy protection and confidentiality observed by HME when handling your personal data (the information shared includes identifiers, commercial information, financial and transaction data, protected information, internet or other similar network activity, professional or employment-related information and non-public education information).
- 7.1.3. **Resellers and agents.** We may share personal data with, and receive personal data from, our dealers, distributors, agents and resellers in order to fulfil orders and facilitate repairs of faulty HME products (the information shared includes identifiers, commercial information and financial and transaction data).
- 7.1.4. **Third party involved in a business transaction.** We may share personal data with one or more third parties in connection with or during negotiation of any merger, financing, acquisition or dissolution, transition, or proceeding involving the sale, transfer, divestiture, or disclosure of all or a portion of our business or assets. In the event of an insolvency, bankruptcy or receivership, such personal data may also be transferred as a business asset. If another company acquires any of our companies, businesses or assets, that acquiring company may acquire your personal data, and in that case, we will inform you of the new controller responsible for the protection of your personal data. We do not guarantee that any entity receiving such data in connection with one of these transactions will comply with all of the terms of this Statement following such transaction. However, it is our practice to seek reasonable protection for personal data in these types of transactions (the information shared may include identifiers, commercial information, financial and transaction data, internet or other similar network activity, professional or employment-related information and non-public education information).
- 7.1.5. **Our advisors.** We may share your personal data with our auditors, legal advisors, and similar third parties in connection with our receiving their professional services, subject to standard confidentiality obligations (the information shared may include identifiers, commercial information, financial and transaction data, internet or other similar network activity, professional or employment-related information, non-public education information and sensitive personal information).

- 7.1.6. **Law enforcement.** We may disclose personal data to the government or to third parties under certain circumstances when legally obligated to do so, such as in connection with suspected illegal activity concerning our Websites, products or services, or to respond to a subpoena, court order or other legal processes, or that we believe may aid a law enforcement investigation. In accordance with applicable law, we reserve the right to release personal data to law enforcement or other government officials, as we, in our sole discretion, deem necessary or appropriate (the information shared may include any category of information we collect).
- 7.1.7. **Legal processes.** We may share all types of personal data with others as required by, or permitted by, applicable law. This may include sharing personal data with governmental entities, or third parties in response to subpoenas, court orders, other legal processes, or as we believe is necessary to exercise our legal rights, to defend against legal claims that have been brought against us, to defend against possible legal claims that we determine in our sole discretion might be brought against us, to investigate and help prevent security threats, fraud or other malicious activity and to protect the rights or personal safety of HME employees and third parties (the information shared may include all categories of information we collect).
- 7.1.8. **Other Third Parties.** We may share aggregated and/or anonymized data with other third parties that are not described above. When we do so, we will either aggregate or anonymize the data so that a third party cannot link data to you, your computer, or your device. Aggregation means that we combine the information of numerous people together so that the data does not relate to any one person. Anonymization means that we remove or change certain pieces of information in such a way that the you are no longer identifiable.

8. Your rights as a data subject

8.1. General rights

- 8.1.1. If any of the personal data that we have about you is incorrect, or you wish to have personal data removed from our records, please contact us using the contact details provided above, or log into your account where relevant.
- 8.1.2. Additionally, if you prefer not to receive marketing messages or information about vacant job positions from us, please let us know by clicking on the unsubscribe link within any such message that you receive, or by sending a message to us using the contact details above. You are able to opt-out of receiving marketing messages from us. However, you cannot opt-out of receiving all emails from us, such as emails about the status of your account or the status of an order for a product you have placed with us.

8.2. European data subject rights

If you are a resident of the European Union or the United Kingdom, you may have the following rights in relation to your personal data in certain circumstances:

- 8.2.1. **Request access to your personal data.**
- 8.2.2. **Request correction of your personal data.**
- 8.2.3. **Request erasure of your personal data.**

- 8.2.4. **Request restriction of processing your personal data.**
- 8.2.5. **Request transfer of your personal data.**
- 8.2.6. **Right to object to the processing of your personal data.**
- 8.2.7. **Right to withdraw consent to the processing of your personal data.**
- 8.2.8. **Right to complain.**

Exercising your rights

To exercise the above-mentioned rights, or to raise a question, comment or complaint, send an email with an enclosed copy of the front side of your identity card, driving license or passport to the Privacy Team at the relevant HME data controller using the contact details above. We reserve the right to request the provision of additional information necessary to confirm the identity of the enquirer.

Lodge a Complaint

You also have the right to lodge a complaint with a data protection authority for your country or region or where an alleged infringement of applicable data protection laws occurs. For the EEA, a list of the national data protection authorities can be found at https://edpb.europa.eu/about-edpb/about-edpb/members_en. For the UK, you have the right to lodge a complaint with the Information Commissioner's Office.

Segmentation and Automated Decision Making

We do not use segmentation or automated decision-making without human intervention, including profiling.

8.3. Privacy rights for residents of California only

Shine the Light Under California law, a California customer with whom HME has an established relationship has the right to request certain information with respect to the types of personal data that we have shared with third parties for direct marketing purposes and the identities of those third parties during the prior calendar year.

Exercising your rights

To exercise your Shine the Light rights, or to raise a question, comment or complaint, send an email with an enclosed copy of the front side of your identity card, driving license or passport to the Privacy Team at the relevant HME data controller using the contact details above. We reserve the right to request the provision of additional information necessary to confirm the identity of the enquirer.

8.4. California Consumer Privacy Act as amended by the California Privacy Rights Act Rights (referred to as "CCPA") for residents of California only

The CCPA provides "consumers" (California residents) with specific rights regarding their "personal information." This section describes your CCPA rights and explains how to exercise those rights.

During the previous twelve (12) months, we have collected the categories of personal information listed in Section 3 of this Statement, used the categories of personal information listed in Section 4 of this Statement, and disclosed the categories of personal information listed in Section 10 of this Statement for a business purpose.

Processing Sensitive Personal Information

We collect and process Sensitive Personal Information for the purposes disclosed at the time we collect this information from our customers, California employees, job applicants or vendors. We do not process this information for purposes other than the purpose for which it was originally collected unless required by law. We use and process Sensitive Personal Information collected from California employees, job applicants or vendors (including racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status) to comply with laws including anti-discrimination laws and disability accommodation laws. We use Sensitive Personal Information from other consumers through our customers (including racial or ethnic origin, religious beliefs, mental or physical health diagnosis, sexual orientation, or citizenship or immigration status) to provide disability accommodations.

Sale of personal information

We do not sell personal information for monetary consideration but we may transfer your information to a third party that provides us with services such as helping us with advertising, data analysis and analytics, and security, which may fall under the definition of for “other valuable consideration” and which may therefore be considered a “sale” under the CCPA. In the preceding twelve (12) months, HME has sold the following categories of personal information:

- 8.4.1. Identifiers;
- 8.4.2. Commercial information;
- 8.4.3. Internet or other similar network activity;
- 8.4.4. Professional or employment-related information;
- 8.4.5. Non-public education information; and
- 8.4.6. Inferences drawn from other personal information.

Sharing personal information for cross-context or behavioral marketing purposes.

We do not share personal information with third parties who may use it for cross-context or behavioral advertising purposes.

Your rights and choices

Verified California residents have the right to obtain certain information about our collection and use of personal information over the past twelve (12) months, including:

- 8.4.7. The categories of personal information we collect;
- 8.4.8. The categories of sources of personal information we collect;

- 8.4.9. Our business purpose for collecting or sharing that personal information;
- 8.4.10. The categories of third parties with whom we share that personal information;
- 8.4.11. The specific personal information we have collected about you over the past twelve (12) months, or, at your option since January 1, 2022 (“Data Portability”);
- 8.4.12. If we sold or disclosed your personal information for a business purpose, two separate lists disclosing:
 - the categories of personal information sold and the category of third party recipients; and
 - list of the categories of personal information that we disclosed for a business purpose.

You have the right to request that we correct information about you that is not correct, to request that we do not sell personal information about you, to request that we do not process sensitive personal information about you for any purposes other than those for which the information was originally collected, and to request that we delete (and direct our service providers to delete) your personal information subject to certain exceptions.

Exercising Personal Information Sales Opt-Out and Opt-In Rights; Limit Processing of Sensitive Information Opt-out

You have the right to direct us to not sell your personal information at any time (the "right to opt-out"). We do not sell or share the personal information of individuals we actually know are less than sixteen (16) years of age. To exercise the right to opt-out, you (or your authorized representative) may submit a request to us by visiting the following page: [Do Not Sell My Personal Information](#). You may exercise this right at any time.

You may also opt out by activating a user-enabled global privacy control, such as a browser plug-in or privacy setting, device setting, or other mechanism, that communicates or signals your choice to opt-out of the sale of personal information. When we receive such a signal we will stop setting third party, analytics, or advertising partner cookies on your browser. This will prevent the sale of information relating to that specific device through cookies to our advertising or analytics partners. This option does not stop all sales of your information because we cannot match your device's identification or internet protocol address with your personally identifiable information like your name, phone number, email address or ZIP Code. If you delete cookies on your browser, any prior do not sell or do not share signal is also deleted and you should make sure that your user-enabled setting is always activated.

Once you make an opt-out request, we will wait at least twelve (12) months before asking you to reauthorize personal information sales.

We do not share personal information for behavioral or cross-context marketing purposes and do not process sensitive personal information for purposes other than those for which it was originally collected.

Exercising your rights for Information Collection or Disclosure Practices, Data Portability, Correction or Deletion

You can exercise any of these rights by contacting us using the contact details set out above or you may submit a request to us by visiting the following page privacy@hme.com. In certain instances, we may have your information because the information is provided to us by our customers for processing. In those circumstances, we may direct you to contact the customer directly to exercise your rights. You may also call us on the following toll free telephone number: [800-978-3514](tel:800-978-3514). You may make a request for Information Collection or Disclosure Practices or Data Portability up to twice within a twelve (12) month period; the disclosure we provide will cover the twelve (12) months prior to your request or, at your option, since January 1, 2022. You may make deletion or correction requests at any time.

We will ask you for information that allows us to reasonably verify your identity (that you are the person about whom we collected personal information) and we will use that information only for that purpose. We may request that you submit a signed statement under penalty of perjury that you are the individual you claim to be. We cannot respond to your request or provide you with personal information if we cannot verify your identity and confirm that the personal information relates to you.

Response timing and format

We will acknowledge receipt of your request for information collection or disclosure practices, data portability, correction or deletion within ten (10) business days and will endeavor to respond within forty-five (45) days of receipt of your request, but if we require more time (up to an additional forty-five (45) days) we will notify you of the reason and extension period in writing.

For requests that we not sell or share your information or limit processing of Sensitive Personal Information we will comply with your request promptly, and at least within fifteen (15) business days.

Where you request a copy of your personal information, we will endeavor to provide the information in a format that is readily useable, including by mailing you a paper copy or providing an electronic copy.

We do not charge a fee to process or respond to your request unless it is excessive, repetitive, or manifestly unfounded. If we determine that the request warrants a fee, we will tell you why we made that decision and provide you with a cost estimate before completing your request. We will not discriminate against you as a result of your exercise of any of these rights.

8.5. Notice to Nevada Residents.

If you would like to tell us not to sell your information please email us at privacy@hme.com with your name, postal address, telephone number and email address with "Nevada do not sell" in the subject line.

8.6. Privacy Rights for Canadian Residents

If you are a resident of Canada, you may have the following rights in relation to your personal data:

8.6.1. **Request access to your personal data and receive information about how it has been processed.**

8.6.2. **Request correction of your personal data.**

8.6.3. **Request erasure of your personal data in limited circumstances.**

8.6.4. **Right to withdraw consent.**

8.6.5. **Right to complain.**

Exercising your rights

To exercise the above-mentioned rights, or to raise a question, comment or complaint, send an email to the Privacy Team at the relevant HME data controller using the contact details above. We reserve the right to request the provision of additional information necessary to confirm the identity of the enquirer.

9. Safety and Confidentiality

- 9.1. HME takes steps to maintain the security of your personal data and to prevent unauthorized access to it through the use of appropriate technology and internal procedures. No method of transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, we cannot guarantee its absolute security and encourage you to use website and share information with caution.
- 9.2. If you choose a direct payment gateway to complete your purchase, then PayPal Gateway stores your credit card data. PayPal Gateway is encrypted through the Payment Card Industry Data Security Standard ("PCI-DSS"). All direct payment gateways adhere to the standards set by PCI-DSS as managed by the PCI Security Standards Council, which is a joint effort of brands like Visa, MasterCard, American Express and Discover. PCI-DSS requirements help ensure the secure handling of credit card information by our store and its service providers.