Subject: **GEA Data Privacy Policy**	Original Effective Date: **October 31, 2022** Revision Date: N/A	

GE Appliances ("GEA")

Data Privacy Policy

Issued by: GEA Data Privacy Steering Committee

Original Issue Date: October 31, 2022

Revision Date: N/A

Policy Owner: GEA General Counsel

Subject: **GEA Data Privacy Policy**	Original Effective Date: **October 31, 2022** Revision Date: N/A	

TABLE OF CONTENTS

1.0 Scope

This Policy describes the privacy-related principles to be followed by individuals handling Personal Data on behalf of GEA, including employees, contractors, and contracted service providers. This Policy applies to Personal Data in any media, including electronic, audio and video recordings, and physical (paper documents, photographs, tapes). It applies to all GE Appliances entities and affiliates ("GEA" or the "Company").

2.0 Purpose and Overview

This Policy establishes the privacy principles to be followed when processing Personal Data of GEA's consumers, customers, vendors, employees and their families, job applicants, and others who work for or visit GEA. Based on recognized data protection practices, these principles are meant to protect both GEA and the Data Subjects whose Personal Data GEA uses in its business. Following the principles supports GEA's efforts to comply with regulatory requirements and abide by industry norms. Failure to follow the principles risks substantial harm to GEA's business and reputation, as well as to the Data Subjects, who may experience embarrassment, inconvenience, and fraudulent use of the information. Protecting the confidentiality and integrity of Personal Data is a critical responsibility of GEA. Compliance with this Policy is mandatory.

The purposes of the Policy are to:
Define Personal Data,
Establish general principles for properly handling Personal Data, and
Assign accountability at GEA for protection of Personal Data.

3.0 Overview of Roles and Responsibilities

GEA Legal is responsible for creating the content of and for revising the Policy.

The GEA Data Privacy Steering Committee is responsible for review and approval of the Policy and revisions thereto.

The Functional leaders are responsible for implementation of and overseeing compliance with the Policy in their respective functional areas.

GEA employees, GEA contractors, and GEA service providers handling Personal Data on behalf of GEA are responsible for complying with the Policy.

4.0 Risk Definition and Strategy

The Policy is intended to protect GEA against legal, reputational, and financial risks. Individuals' rights to the privacy of their Personal Data are subject to stringent regulations.

Failure by GEA to abide by regulatory requirements can lead to investigations and litigation and to the imposition of fines, penalties, and monetary damages. GEA handles Personal Data belonging to a range of individuals, including GEA consumers, employees, customers, and suppliers. Failure by GEA to protect and use appropriately the Personal Data of these stakeholders can tarnish GEA's reputation as a responsible steward of the Personal Data and can harm the value of GEA's brand. GEA relies on the trust of its consumers, employees, and business partners to succeed. If GEA loses this trust it can negatively impact the Company's relationship with these stakeholders and, ultimately, its financial performance.

Creation, implementation, and enforcement of this Policy establishes a framework for GEA to address risks associated with processing Personal Data in its business operations. Adherence to the Privacy Principles can diminish the likelihood of regulatory infractions and attendant enforcement actions and litigation. Employing appropriate Personal Data handling practices can bolster trust in GEA and its products. Avoiding missteps in processing Personal Data protects the Company's assets and reputation, as well as potential setbacks in its financial performance.

5.0 Definitions

"Data Subject" means the individual whose Personal Data is collected or processed.

"Personal Data" means information the Company has collected or otherwise has in its possession that (i) identifies, (ii) can be used by itself or in combination with other data to identify an individual, or (iii) that otherwise relates to an individual, such as:

- Names
- Addresses
- Telephone numbers
- Email addresses
- Employee identification numbers

Certain Personal Data, known as **"Sensitive Personal Data",** if lost, compromised, or improperly disclosed or accessed could result in harm, embarrassment, inconvenience, or unfairness to an individual and therefore is subject to heightened protections. Examples of Sensitive Personal Data include:

- An individual's government-issued identification number, including a social security number, driver's license number, or state-issued identification number
- A financial account number, credit card number, or debit card number that would permit access to an individual's financial account
- Biometric, medical, health, or health insurance information
- Precise geolocation data
- Racial or ethnic origin

Deleted: ¶
GEA maintains a listing of categories of Data Subjects. ¶
See list (VPN required).¶

"Privacy Incident" means (i) any loss of or unauthorized access, disclosure, or acquisition of Personal Data, (ii) any collection, use, sharing, or processing of Personal Data that does not conform to this Policy or other GEA policies for handling Personal Data or (iii) is inconsistent with GEA's legal or contractual obligations.

Deleted: GEA maintains a listing of all Personal Data and Sensitive Personal Data elements it uses. ¶ See list (VPN required).¶

6.0 Policy

The Company will process Personal Data strictly in accordance with the following Privacy Principles:

Principle 1: Lawfulness, fairness, and transparency
Whenever the Company collects Personal Data for any purpose it must inform the Data Subject of how the data will used, processed, disclosed, protected, and retained. This notification must be presented at or before the point of collection or use of the data. Where required, GEA will obtain the individual's consent prior to collecting the data. GEA will process Personal Data only in compliance with applicable Company policies, notices, and applicable laws and only for legitimate business purposes.

Principle 2: Purpose limitation
The Company will process Personal Data only in accordance with the purposes notified to the individual at the time of collection. GEA will process Personal Data only to the extent necessary to accomplish the Company's legitimate business purposes or as necessary to comply with law. GEA will not further process Personal Data in a manner that is incompatible with those purposes.

Principle 3: Data minimization
GEA will collect only such Personal Data as is adequate, relevant, and limited in scope to achieve the purposes notified to the Data Subjects.

Principle 4: Access, use, and sharing of Personal Data
GEA personnel may access Personal Data only to the extent the information relates to and is necessary to perform assigned job duties. GEA personnel are not permitted to use Personal Information in ways that are incompatible with the notice given to the Data Subject at the time the information is collected. Personal Data may be shared with another Company employee, agent, or representative only if the recipient has a job-related need to know the information. Personal Data may be shared with a Third-Party Service Provider or other GEA business partner only where the third party has a need to know the information for the purpose of providing the contracted services or other business purposes agreed by GEA. Shared Personal Data must be used in compliance with the privacy notice provided to the Data Subject. Personal Data may not be shared unless the third party agrees in writing to handle the data in a manner consistent with this Policy.

Principle 5: Data subject rights
GEA enables Data Subjects to exercise legal rights related to how GEA handles their Personal Data. These rights vary depending on the relevant jurisdiction, but may include:

The right to know what Personal Data the Company maintains about the individual and with whom the Company has shared the Personal Data
The right to access or correct the Personal Data
The right to delete or limit the use of the Personal Data

GEA personnel who seek information about applicable legal requirements or who receive a request or complaint from a Data Subject regarding the handling of the Data Subject's Personal Data should contact the Legal business partner for their area.

Principle 6: Accuracy
GEA will collect, maintain, and use Personal Data that is accurate, complete, and, where necessary, kept up to date. The Company will take steps to ensure that Personal Data found to be inaccurate is promptly erased or rectified.

Principle 7: Security
GEA is responsible for protecting Personal Data it processes. The Company has implemented an Information Security Program ("ISP") that sets forth technical, administrative, and physical safeguards to protect the confidentiality, integrity, and availability of Personal Data. GEA will follow the security procedures set out in the ISP to protect all Personal Data from loss, misuse, unauthorized access, and unauthorized disclosure.

Principle 8: Retention and disposal
GEA will keep Personal Data for no longer than is necessary to fulfill the legitimate business purpose for which it was collected or to satisfy a legal requirement. The Company will follow the applicable records retention schedules and policies and dispose of any media containing Personal Data in accordance with the applicable records management policy.

Principle 9: Accountability
GEA is responsible for, and able to demonstrate compliance with, the Privacy Principles set forth in this Policy. GEA will develop and maintain procedures consistent with the Privacy Principles that can be used to demonstrate GEA's compliance with the principles.

7.0 Training and Awareness

All Company personnel who have access to Personal Data are to be trained on this Policy and the treatment of Personal Data. Personnel with responsibility for supervising employees or

managing Third-Party Service Provider relationships should be trained on supervision over those employees and Third-Party Service Providers

8.0 Roles and Responsibilities

Roles and responsibilities are set forth in Appendix 1.

9.0 Policy Exceptions and Escalations

Functional leaders will be responsible for assessing their areas and identifying any areas of potential non-compliance under this Policy. It is expected that requests by Functional Leaders to be exempt from any areas to this Policy will be rare. Any areas of potential non-compliance must be highlighted to the Policy Owner/Contact within one month from the issuance date or re-approval of this Policy.

Following the determination of non-compliance:

- The Functional leader is required to establish an action plan agreed with the Policy Owner. These plans must be documented with a clear timeline for closure and an identified responsible party to oversee implementation of the action plan; or
- The Policy Owner grants the Function an exception, with rationale clearly documented and maintained by the Policy Owner.

The Policy Owner will report a summary of all exceptions granted to the Data Privacy Steering Committee at least quarterly and the summary will be available to the Director for Compliance to assess trends and patterns regarding Policy effectiveness.

10.0 Violations of this Policy

Violations of this Policy can signify internal risk management weaknesses, which may result in supervisory criticism, regulatory penalties, and adverse publicity. Violations also may subject employees to disciplinary action up to and including termination. Violations of this Policy must be reported via one of the means authorized in the Compliance and Integrity portal.

Managers who become aware of violations of this Policy must also submit a Privacy Incident Report via the Privacy Incident portal.

If local law restricts disclosure, escalation shall be done in a manner consistent with such law.

Formatted: Indent: Left: 0", First line: 0"

Deleted: following

Deleted: :¶
¶
1. In-person, by contacting your supervisor, Business Compliance Leader, HR leader, persons in Finance or Legal, EHS, or an Ombuds person. ¶
2. Submit a concern through the Concern Reporting – Manager's tool, available on the GEA Connect Homepage, ABC Menu, "C". ¶
3. Anonymously, via the Ombuds icon on your desktop, the GEA Homepage – My Links "O" Ombuds Portal, or through the toll-free hotline at 1-866-585-1263. ¶
4. Text message (North America only) – To report an anonymous message, open a new text message on your cell phone, and enter "274637" in the "To" field, then start your text with the word OMBUDS followed by a space in the body of the message. ¶
5. GEA's Secure Avenue for Everyone (SAFE) tool – anonymously report concerns directly to your Ombuds person from any computer at any time via ombuds.geappliances.com.

Deleted: Privacy Incident

11.0 Policy Review

The Data Privacy Steering Committee must approve this Policy at least every three years and the Policy Owner is responsible for approving all material changes to it and its appendices. Evidence of review and approval of this Policy shall be documented.

APPENDIX 1

Roles and Responsibilities

1. Data Privacy Steering Committee

The responsibilities of the Steering Committee are as follows:

- Reviewing and approving the Policy at least every three years
- Ensuring the implementation of this Policy by the Functions
- Receiving semi-annual reporting on material policy exceptions or violations from the Policy Owner
- Monitoring trends with policy exceptions
- Ensuring that competent and qualified personnel manage and are accountable for the processes necessary to ensure compliance with this Policy

2. Functional leaders

The responsibilities of the GEA functional leaders are as follows:

- Enforcing compliance with this Policy
- In conjunction with the Steering Committee and the Chief Privacy Officer, designating individuals to assist with development and drafting of Functional policies, processes, or standards
- Communicating the creation or revision of Functional policies, processes, or standards to affected employees

3. Policy Owner

The responsibilities of the Policy Owner are as follows:

- Exercising ultimate responsibility for coordinating with the Chief Privacy Officer to ensure data privacy-related policies are drafted, reviewed, approved, and maintained in accordance with this Policy
- Communicating the approval of data privacy-related policies to affected employees, summarizing their content, highlighting awareness, and training requirements, and communicating any changes to existing policies through bulletins, procedures, standards, or leading practices
- Escalating policy exceptions to the Steering Committee

Deleted: **Related Policies**¶
¶
Data and Document Classification Guidelines¶
¶
Document Management¶
¶
Acceptable Use of GEA Information Resources¶
¶
GEA Information Security Policy¶
¶
GEA IT PII Management Procedure¶
¶
GEA Data Protection Standard¶
¶
Web Address¶
¶
<Insert web address here>¶
Page Break
¶

APPENDIX 2

Glossary

Function – refers to the major infrastructure support units as defined by GEA. These are: Commercial, Technology, Supply Chain, Distribution & Services, Finance, Marketing, Sales, Human Resources, Digital Technology, Legal, Communications, and Microenterprises.

Function Leader – Executive of the major infrastructure support unit as defined by GEA.

Guidance - Counseling, help, advice, interpretation, or instruction to further clarify, expand, or enhance Policy.

Leading Practice -- a process, practice or solution judged as the preferred way to reach a goal or result; held up as a model to be learned from or followed. Note that Leading Practices are not auditable or enforceable because they represent aspirational activities or ways in which policy requirements could be met. These may include activities or practices adopted by industry leaders but not yet or required to be, adopted by GEA.

Procedure -- a written set of steps to execute policies through specific, prescribed actions. Procedures tend to be more detailed than policies. They identify the method and state in a series of steps of exactly "how" to accomplish an intended task, achieve a desired business or functional outcome and execute the policy.

Process -- a series of related steps, activities or tasks that produce a specific service or product for a customer, or implement key activities, steps, or tasks for a Function to manage, measure, monitor, or report on risks (e.g., accounting, risk management, technology, compliance). It often can be visualized with a flowchart, with mapping of a sequence of activities.

Standard – A clarifying or interpretive document that contains counseling, help, advice, interpretation, requirements, or instruction to further clarify, expand, or enhance Policies.