

Garmin Employee Privacy Shield Policy

Last updated:

Overview

Garmin International, Inc., Garmin Services, Inc., and Garmin AT, Inc. (collectively the “Covered Garmin Entities” or “Garmin”) comply with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of Personal Data transferred from the European Union (“EU”) member countries, the United Kingdom (“UK”), and Switzerland to the United States. The Covered Garmin Entities have certified to the U.S. Department of Commerce that they adhere to the EU-U.S. Privacy Shield Principles and the Swiss-U.S. Privacy Shield Principles (collectively, the “Privacy Shield Principles”) with respect to Personal Data that they receive from the EU, UK, or Switzerland in reliance on the Privacy Shield.

Garmin developed this Employee Privacy Shield Policy (“Policy”) to provide Employees with information about how Garmin implements the Privacy Shield Principles with respect to Employee Personal Data. In the unlikely event that there is any conflict between the terms in this Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. Employees can learn more about the Privacy Shield program [here](#) and view the Privacy Shield List [here](#).

Definitions

For purposes of this Policy:

“Controller” means a person or organization which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.

“Employee” means any current, former, or prospective employee, temporary worker, intern, or other non-permanent employee of Garmin or any Garmin affiliate, who is located in the EU, UK, or Switzerland.

“EU” means the European Union and Iceland, Liechtenstein, and Norway.

“Personal Data” means data about an identified or identifiable individual that is recorded in any form and received by Garmin in the United States from the EU, UK, or Switzerland.

“Privacy Shield Principles” means the Principles and Supplemental Principles of the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework.

“Processing” means any operation or set of operations which is performed upon Personal Data, whether or not by automated means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure or dissemination, and erasure or destruction.

“Processor” means any natural or legal person, public authority, agency, or other body that Processes Personal Data on behalf of a Controller.

“Sensitive Data” under the EU-U.S. Privacy Shield Framework means Personal Data specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information specifying the sex life of the individual.

“Sensitive Data” under the Swiss-U.S. Privacy Shield Framework means Personal Data specifying medical or health conditions, personal sexuality, racial or ethnic origin, political opinions, religious, ideological or trade union-related views or activities, or information on social security measures or administrative or criminal proceedings and sanctions, which are treated outside pending proceedings.

Privacy Shield Principles:

Garmin’s adherence to the following Privacy Shield Principles provides the necessary level of protection required for the transfer of Employee Personal Data outside of the EU and Switzerland.

Notice

Garmin provides Employees with a privacy policy, which notifies Employees about Garmin’s practices concerning Employee Personal Data, including the types of Employee Personal Data that Garmin collects; the purposes for which it collects and uses Employee Personal Data; the types of third parties to which Garmin discloses Employee Personal Data and the purposes for doing so; the rights and choices Employees have for limiting the use and disclosure of their Employee Personal Data; and how to contact Garmin about its practices concerning Employee Personal Data. A copy of the Information Notice Concerning the Processing of Personal Data for Employees in your office has been provided to you and can be obtained from the Human Resources (“HR”) manager for your office or the EMEA HR manager. Other information required by the Privacy Shield Notice Principle is provided to Employees in this Policy.

Choice

Garmin provides Employees with the opportunity to choose how their Employee Personal Data may be used under certain circumstances. If Employee Personal Data is to be used for a new purpose that is materially different from that for which the Employee Personal Data was originally collected or subsequently authorized, or if the Employee Personal Data is to be disclosed to a third-party Controller, Garmin will provide Employees with an opportunity to choose whether to have their Employee Personal Data so used or disclosed. Requests to opt out of such use or disclosure should be sent to the Employee’s HR Manager. If Sensitive Personal Data is collected and will be used for a new purpose that is different from that for which the Sensitive Personal Data was originally collected or subsequently authorized, or is to be disclosed to a third party, Garmin will obtain the Employee’s affirmative express consent prior to such use or disclosure.

However, Garmin may disclose Employee Personal Data without offering an opportunity to opt out, subject to applicable employment laws: (a) When sharing Employee Personal Data with third-party Processors that Garmin has retained to perform services on its behalf and pursuant to its

instructions; (b) When making promotions, appointments, or similar employment decisions; or (c) In response to lawful requests by public authorities, including to meet national security, public interest, or law enforcement requirements.

Accountability for Onward Transfer

Garmin will only transfer Employee Personal Data to a third party acting as a Controller, other than to a third-party Controller for occasional employment-related operational needs, if the third-party Controller has provided contractual assurances that it will: (a) Process Employee Personal Data in a manner consistent with all applicable requirements of the Privacy Shield Principles; (b) Process Employee Personal Data only for limited and specified purposes and in accordance with the consent provided by the relevant Employee; (c) Provide at least the same level of protection for Employee Personal Data as is required by the Privacy Shield Principles; and (d) Promptly notify Garmin and immediately cease processing Employee Personal Data (or take other reasonable and appropriate remedial steps) if the third-party Controller determines that it cannot meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles.

Garmin will only transfer Employee Personal Data to a third-party Processor for limited and specified purposes, and only if the third-party Processor has provided contractual assurances that it will: (a) Process the Employee Personal Data in a manner consistent with the Privacy Shield Principles and only for limited and specified purposes set forth in documented instructions from Garmin; (b) Refrain from transferring Employee Personal Data to any person or entity without Garmin's written authorization; (c) Taking into account the nature of the Processing, assist Garmin in responding to Employees exercising their rights under the Privacy Shield Principles; (d) Provide at least the same level of privacy protection for Employee Personal Data as is required by the Privacy Shield Principles; (e) Provide appropriate technical and organizational measures to protect Employee Personal Data against accidental or unlawful destruction or accidental loss, alteration, and unauthorized disclosure or access; and (f) Promptly notify Garmin and immediately cease processing Employee Personal Data, or take other reasonable and appropriate remedial steps, if the Processor determines that it cannot meet its obligation to provide the same level of protection as is required by the Privacy Shield Principles.

Security

Garmin takes reasonable and appropriate measures to protect Employee Personal Data from loss, misuse and unauthorized access, disclosure, alteration and destruction, taking into account the risks involved in the Processing and the nature of the Employee Personal Data.

Data Integrity and Purpose Limitation

Garmin limits the collection of Employee Personal Data to information that is relevant for the purposes of Processing. Garmin does not Process Employee Personal Data in ways that are incompatible with the purposes for which the information was collected or subsequently authorized by the relevant Employee. In addition, Garmin takes reasonable steps to ensure that the Employee Personal Data it Processes is reliable for its intended use, and is accurate, complete, and current. In this regard, Garmin relies on its Employees to update and correct their Employee Personal Data to the extent necessary for the purposes for which the information was collected or subsequently

authorized by the Employees. Employees should contact their Human Resources Manager with any requests that Garmin correct or update their Employee Personal Data.

Garmin takes reasonable and appropriate measures to retain Employee Personal Data in a form that identifies or renders identifiable the relevant Employee only for as long as it serves a purpose of Processing that is compatible with the purposes for which the Employee Personal Data was collected or subsequently authorized by the Employee. Garmin will adhere to the Privacy Shield Principles for as long as it retains such Employee Personal Data.

Access

Garmin provides Employees with reasonable access to the Employee Personal Data that Garmin maintains about them. Garmin also provides Employees with a reasonable opportunity to correct, amend, or delete their Employee Personal Data, as appropriate, where the Employee Personal Data is inaccurate, or an Employee believes that his or her Employee Personal Data has been processed in violation of the Privacy Shield Principles, except where the burden or expense of providing access would be disproportionate to the risks to your privacy or where the rights of other individuals would be violated.

Requests for access, correction, amendment, or deletion of Employee Personal Data should be directed to the Employee's HR Manager or to the Local Data Privacy Champion ("LDPC") for their office or region.

Recourse, Enforcement and Liability

In compliance with the Privacy Shield Principles, Garmin conducts an annual self-assessment of its relevant Privacy Shield practices, which includes verifying that the attestations and assertions that Garmin makes about its Privacy Shield practices are true, and that Garmin's Privacy Shield practices have been implemented as represented and in accordance with the Privacy Shield Principles. Garmin also engages in training to support compliance with this Policy and the Privacy Shield Principles.

Garmin is committed to resolving questions and complaints about its collection and use of Employee Personal Data. Employees with questions or complaints regarding Garmin's collection or use of Employee Personal Data should contact their HR Manager or the LDPC for their office or region. Garmin will investigate any issues raised and will seek to resolve any complaints or disputes regarding its collection or use of Employee Personal Data in accordance with the principles contained in this Policy.

If an Employee complaint cannot be resolved through Garmin's internal processes, Garmin will cooperate with an EU Data Protection Authority ("DPA") or the Swiss Federal Data Protection and Information Commissioner ("Commissioner"), as appropriate, and will comply with the advice given by the DPA and/or the Commissioner relating to Employee Personal Data transferred from the EU, UK, or Switzerland. If Garmin does not address an Employee Personal Data complaint to an Employee's satisfaction, an Employee can request additional information or file a complaint, free of charge, with the DPA in his or her EU Member State, the Commissioner in Switzerland, or the Information Commissioner's Office ("ICO") in the UK. Contact information for the DPAs, the Commissioner, and the ICO is available [here](#).

Employees also may, under certain circumstances, invoke binding arbitration for complaints regarding Privacy Shield compliance that are not able to be resolved by any other means. More information about the Privacy Shield binding arbitration option is available [here](#).

Garmin is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission and will remain responsible, under the Privacy Shield Principles, if any of its third-party Processors Process Employee Personal Data in a manner inconsistent with the Privacy Shield Principles, unless Garmin proves it is not in any way responsible for the event giving rise to the damage.

Changes to this Policy

This Policy may be amended from time to time, consistent with the requirements of the Privacy Shield Principles. Employees can determine when this Policy was last revised by referring to the “Last Updated” legend at the top of the first page of the Policy. Any changes will become effective when the revised Policy is published on Garmin’s Intranet. Garmin will provide specific notice to Employees via email of the revised Policy if changes to the Policy are material.

How to Contact Garmin

If you have any questions concerning this Policy or Garmin’s Privacy Shield practices, you may send any such questions via email to Garmin’s EU DPO at euprivacy@garmin.com.