
nGuard EU-US Privacy Shield Policy

Overview

nGuard Inc. complies with the EU-US Privacy Shield Framework as set forth by the US Department of Commerce regarding the collection, use, and retention of personal information from European Union member countries. nGuard has certified that it adheres to the Privacy Shield Principles. If there is any conflict between the policies in this privacy policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view our certification, please visit <https://www.privacyshield.gov/>

Definitions

“Data Subject” means the individual to whom any given Personal Data covered by this Privacy Shield Policy refers.

“Personal Data” means any information relating to an individual residing in the European Union that can be used to identify that individual either on its own or in combination with other readily available data.

“Sensitive Personal Data” means Personal Data regarding an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, physical or mental health, or sexual life.

Scope and Responsibility

This Privacy Shield Policy applies to Personal Data or Sensitive Personal Data transferred from European Union member countries to nGuard's operations in the U.S. Although nGuard does not collect Personal Data or Sensitive Personal Data from EU citizens, this policy serves as guidance if such collection takes place at any point in the future.

All employees of nGuard that have access in the U.S. to Personal or Sensitive Personal Data covered by this Privacy Shield Policy are responsible for conducting themselves in accordance with this Privacy Shield Policy. Adherence by nGuard to this Privacy Shield Policy may be limited to the extent required to meet legal, regulatory, governmental, or national security obligations, but Personal Data covered by this Privacy Shield Policy shall not be collected, used, or disclosed in a manner contrary to this policy without the prior written permission of nGuard's Chief Privacy Officer.

**Privacy
Shield
Principles**

nGuard commits to the Privacy Shield's Principles for all Personal Data and Sensitive Personal Data received by nGuard in the U.S. from European Union member countries in reliance on the respective Privacy Shield framework.

1. Notice

nGuard will notify Data Subjects covered by this Privacy Shield Policy about its data practices regarding Personal Data received by nGuard in the U.S. from European Union member countries per the Privacy Shield framework, including the types of Personal Data it collects about them, the purposes for which it collects and uses such Personal Data, the types of third parties to which it discloses such Personal Data and the purposes for which it does so, the rights of Data Subjects to access their Personal Data, the choices and means that nGuard offers for limiting its use and disclosure of such Personal Data, how nGuard's obligations under the Privacy Shield are enforced, and how Data Subjects can contact nGuard with any inquiries or complaints.

2. Choice

If Personal Data covered by this policy is to be used for a new purpose that is materially different from that for which the originally collected or subsequently authorized, or is to be disclosed to a non-agent third party, nGuard will provide Data Subjects with an opportunity to choose whether to have their Personal Data so used or disclosed. Requests to opt out of such uses or disclosures of Personal Data should be sent to: privacy.shield@nGuard.com

If Sensitive Personal Data covered by this Privacy Shield Policy is to be used for a new purpose that is different from that for which the Personal Data was originally collected or subsequently authorized, or is to be disclosed to a third party, nGuard will obtain the Data Subject's explicit consent prior to such use or disclosure.

3. Accountability for Onward Transfer

In the event we transfer Personal Data covered by this Privacy Shield Policy to a third party, we will do so consistent with any notice provided to Data Subjects and any consent they have given, and only if the third party has given nGuard contractual assurances that it will (i) process the Personal Data for limited and specified purposes consistent with any consent provided by the Data Subjects, (ii) provide at least the same level of protection as is required by the Privacy Shield Principles and notify us if it makes a determination that it cannot do so; and (iii) cease processing of the Personal Data or take other reasonable and appropriate steps to remediate if it makes such a determination. If nGuard has knowledge that a third party acting as a controller is processing Personal Data covered by this Privacy Shield Policy in a way that is contrary to the Privacy Shield Principles, nGuard will take reasonable steps to prevent or stop such processing. In cases of onward transfer to third parties of data of EU individuals received pursuant to the EU-US Privacy Shield, nGuard is potentially liable.

**Privacy
Shield
Principles
Cont.**

With respect to transferring personal data to a third party acting as an agent, nGuard will: (i) transfer such data only for limited and specified purposes; (ii) ascertain that the agent is obligated to provide at least the same level of privacy protection as is required by the Principles; (iii) take reasonable and appropriate steps to ensure that the agent effectively processes the personal information transferred in a manner consistent with the organization's obligations under the Principles; (iv) require the agent to notify the organization if it makes a determination that it can no longer meet its obligation to provide the same level of protection as is required by the Principles; (v) upon notice, including under (iv), take reasonable and appropriate steps to stop and remediate unauthorized processing; and (vi) provide a summary or a representative copy of the relevant privacy provisions of its contract with that agent to the Department upon request.

4. Security

nGuard takes reasonable and appropriate measures to protect Personal Data covered by this Privacy Shield Policy from loss, misuse, and unauthorized access, disclosure, alteration, and destruction.

5. Data Integrity and Purpose Limitation

nGuard will limit the collection of Personal Data covered by this Privacy Shield Policy to information that is relevant for the purposes of processing. nGuard does not process such Personal Data in a way that is incompatible with the purposes for which it has been collected or subsequently authorized by the Data Subject. nGuard will take reasonable steps to ensure that such Personal Data is reliable for its intended use, accurate, complete, and current. nGuard will take reasonable and appropriate measures to comply with the requirement under the Privacy Shield to retain Personal Data in identifiable form only for as long as it serves a purpose of processing, which includes nGuard's obligations to comply with professional standards, nGuard's business purposes and unless a longer retention period is permitted by law, and it adheres to the Privacy Shield Principles for as long as it retains such Personal Data.

6. Access

Data Subjects whose Personal Data is covered by this Privacy Shield Policy have the right to access such Personal Data and to correct, amend, or delete such Personal Data if it is inaccurate or has been processed in violation of the Privacy Shield Principles (except when the burden or expense of providing access, correction, amendment, or deletion would be disproportionate to the risks to the Data Subject's privacy, or where the rights of persons other than the Data Subject would be violated). Requests for access, correction, amendment, or deletion should be sent to: privacy.shield@nGuard.com

**Privacy
Shield
Principles
Cont.****7. Recourse, Enforcement, and Liability**

nGuard's participation in the EU-U.S. Privacy Shield Framework is subject to investigation and enforcement by the Federal Trade Commission. In compliance with the Privacy Shield Principles, nGuard commits to resolve complaints about your privacy and our collection or use of your Personal Data. Data Subjects with inquiries or complaints regarding this Privacy Shield Policy should first contact nGuard at: privacy.shield@nGuard.com

nGuard has further committed to refer unresolved privacy complaints under the EU-U.S. Privacy Shield Principles to an independent dispute resolution mechanism, JAMS, a US based, private sector Alternative Dispute Resolution (ADR) Provider. If you do not receive timely acknowledgment of your complaint, or if your complaint is not satisfactorily addressed, please visit <https://www.jamsadr.com/file-an-eu-us-privacy-shield-or-safe-harbor-claim> for more information and to file a complaint.

Under certain conditions detailed in the Privacy Shield, Data Subjects may be able to invoke binding arbitration before the Privacy Shield Panel to be created by the U.S. Department of Commerce and the European Commission. nGuard agrees to periodically review and verify its compliance with the Privacy Shield Principles, and to remedy any issues arising out of failure to comply with the Privacy Shield Principles. nGuard acknowledges that its failure to provide an annual self-certification to the U.S. Department of Commerce will remove it from the Department's list of Privacy Shield participants.

**Changes to
nGuard
Privacy
Shield Policy**

This Privacy Shield Policy may be amended from time to time consistent with the requirements of the Privacy Shield. Appropriate notice regarding such amendments will be given.
