W. L. Gore & Associates

Data protection approach

Our commitment to data privacy and information security

Every day we build upon our foundation of integrity, innovation and sound science as we partner with industry-leading innovators to rapidly create unique and valued products and services. With each interaction, we are collectively committed to creating exceptional experiences and delivering on our promise of *Together, improving life*.

To deliver on our promise, we consciously strive to uphold our legacy of high ethics and integrity through a commitment to individual accountability, fairness and sound global business practices. We live this promise through our commitment to safeguard data (e.g., personal information, intellectual property and confidential/proprietary information) that we process. To enable this commitment, we have developed and implemented a broad set of capabilities related to data privacy and information security.

Overview

Data privacy

We show our commitment to privacy by following established privacy principles that serve as the foundation of how we manage and protect personal information entrusted to Gore.

The Gore Global Privacy Program includes a set of program policies, requirements and support mechanisms that demonstrate our compliance with applicable privacy regulations globally.

PRIVACY

SECURITY

Information security

To enable confidentiality, integrity, availability and resiliency of information assets, our Information Security Program has implemented internal controls based on industry standard security frameworks.

The principles underlying the Information Security Program are designed to promote our responsibility as stewards of the data entrusted to us.

Our principles

Privacy principles

- **Accountability:** Accountable for compliance with applicable privacy requirements
- **Lawfulness:** Personal information (PI) processed in a manner that is lawful and fair
- **Consent:** Permission must be obtained from the individual when required
- **Data transfer:** Consistent with the notice provided
- **Data Quality:** PI must be accurate
- **Purpose specification:** PI processed for specified and explicit purpose
- **Data minimization:** Only PI that is required is collected and processed
- **Security:** PI protected by suitable technical and organizational measures

Information security principles

- **Accountability:** Accountable for compliance with applicable cybersecurity regulations
- **Lawfulness:** Abide by applicable laws
- **Risk-based:** Apply security controls appropriate to the identified risks
- **Security by design**: Apply security controls throughout the entire Software Development Life Cycle (SDLC)
- **Defense in depth:** Layered security controls to ensure multiple levels of protection
- **Alignment:** Align information security program with industry cybersecurity frameworks and best practices
- **Responsible:** Empower associates and partners with awareness training needed to appropriately handle sensitive and confidential information

What does our commitment to data privacy and information security look like?

Gore Global Data Privacy Program key elements

- A Privacy Office to manage our Global Privacy Program with identified roles and responsibilities
- Established policies and procedures that require the appropriate measures to manage and protect personal information
- Privacy training and awareness program to foster a compliant privacy culture
- Privacy by design approach in system/application development lifecycle
- Documented data inventory of how and where personal information is processed
- Managed notice and consent practices when collecting and processing personal information
- Managed individual rights to provide individuals appropriate control of their data
- Privacy and data protection impact assessments to evaluate privacy risk with associated risk mitigation processes
- Third party privacy risk management and the management of cross-border data transfers
- Privacy breach response processes and procedures

Gore Global Information Security Program key elements

- User roles and privileges based on least privilege principle
- Remote access via VPN with multi-factor access
- Centralized user account administration and authentication
- Monitoring of infrastructure technologies by audit logging and event log reviews
- Risk based methodology for third party assessments
- Use of industry standard cryptographic solutions to comply with local laws
- Information assets are encrypted at rest and in transit where feasible
- Established procedures for routine patch and vulnerability management
- Restricted access to information assets from approved media devices only
- Cybersecurity incident response team response processes and procedures
- Intrusion detection and prevention technology to identify and protect from different types of attacks
- Logical and physical segregation of networks based on security requirements
- Anti-malware software updates with the release of new signatures provided by the vendor

Please refer to our Privacy Notice at gore.com/privacy and if you have any questions, see our “Contact Us” page on the website or send an email to dataprivacyoffice@wlgore.com. If you have any questions regarding our information security program, send an email to Gore_Information_Security_Team@wlgore.com.