FORTRA™

FAQ (TRIPWIRE)

Tripwire ExpertOps Data Collection and Processing FAQ, April 2022

1. **What kind of data will be collected during the provision of Fortra's Tripwire® ExpertOps℠ services?**
   a. Business contact information, including name, business address, business phone number, business fax number, business email address for Customer personnel including client administrators.
   b. Electronic identification and access credentials for business-managed assets, including IP address, user name, password.
   c. Log data, configuration data and diagnostic output of business-managed assets.
   d. The purpose of the services is monitoring OS-level files (exe, dll, reg keys, config files, etc) sufficient to support operational integrity of the host and to validate its configuration is secure.
2. **Who owns the data collected under Q.1?**
   - The customer owns the data at all times.
3. **How does Tripwire plan to use such data?**
   - The contact information shall only be used for the purposes of (i) receiving and providing ExpertOps services; (ii) receiving and providing related professional consulting and support services offered by Tripwire; and (iii) processing of payment for the services, where applicable.
4. **Who has access to customer data?**
   - Managed Services Engineers and system administrators if administrators explicitly elevate their rights to access the data.
5. **Where does customer data reside?**
   - Depending on customer location, customer data resides regionally in a cloud data center in the Australia, United Kingdom, United States, Canada, India, Mexico, Singapore, or Vietnam.
6. **Where is customer data stored or processed during the delivery of ExpertOps services?**
   - In the case of information under **Q.1** a: Salesforce. The only contact information in AWS is first name, last name, and (if needed and requested by customer) email address.
   - In the case of information under **Q.1** b: AWS only.
   - In the case of information under **Q.1** c: AWS only.
   - Access to the AWS hosting environment is secured by several layers of physical and information security measures.
7. **Is customer data retained after the termination of ExpertOps services?**
   - Tripwire destroys ExpertOps collected customer data under Q.1 b and c 30 days after termination of the ExpertOps services term or applicable contract, per Tripwire's data retention policy.
   - In the case of information under **Q.1** a, Tripwire will either delete or anonymize it or, if this is not possible (for example, because personal information has been stored in backup archives), then Tripwire will securely store such personal information and isolate it from any further processing until deletion is possible.

8. **Will Tripwire have access to customers' networks during delivery of ExpertOps services?**
   - No. Tripwire will not have interactive login access to any customer systems.
9. **Does Tripwire use overseas subcontractors in the delivery of ExpertOps services?**
   - ExpertOps functions are performed by managed service engineers in the U.S. and in India. The India-based partner works on Tripwire managed systems in the U.S., using secure remote log-in capability.
10. **Can customers receive an export of their console configuration data, file system configuration data, and a backup of their database upon request?**
    - Yes, customers can receive an export of such data within 10 days of the request; provided however where such request is made subsequent to termination of ExpertOps services, the request must be submitted to Tripwire within 30 days of termination of the services.
11. **Will Tripwire be hosting, managing or processing customer PCI data?**
    - Generally no. Tripwire does not store, process, or transmit cardholder data.
    - Depending on how a customer uses ExpertOps services, ExpertOps might be used to monitor IT assets in a PCI environment. If a customer uses ExpertOps to monitor IT assets in a PCI DSS environment, then ExpertOps needs to be PCI DSS compliant (which it is). As part of PCI DSS compliance, we make available the PCI DSS responsibility matrix.
12. **What is Tripwire's standard archival procedures?**
    - Backups are taken nightly and use geo-redundant storage in the US to ensure that data is recoverable regardless of a localized catastrophic event. Backup schedules and retention is as follows:
      - Daily backups are retained for 60 days
      - Weekly backups are retained for 52 weeks
      - Monthly backups are retained for 24 months
13. **Does Tripwire have an SOC 1 or SOC 2 report?**
    - SOC 1 reports are used by service organizations that host financial information that could affect their clients' financial reporting. Tripwire doesn't offer these services.
    - SOC 2 reports are used by service organizations that host other client information. These reports assess the service providers' core controls relating to the security, availability, processing integrity, confidentiality, and privacy. Tripwire has a SOC 2 report inclusive of ExpertOps and Tripwire Anyware™*. This report is available to current and prospective ExpertOps customers under NDA terms.

      *The 2021 report was prior to Tripwire Anyware branding and uses tripwire.io/SaaS language. The 2022 report will use Tripwire Anyware to refer to Tripwire's SaaS offerings.
14. **What other compliance certifications does the Tripwire ExpertOps environment have?**
    - Tripwire is PCI compliant and can also disclose its PCI DSS Attestation of Compliance under an NDA.
15. **Is Tripwire considered a data processor pursuant to the GDPR?**
    - Yes, Tripwire is a processor in relation to the data processing carried out on behalf of Customer in relation to the services provided by Tripwire to Customer under the ExpertOps Service Agreement. Tripwire will enter into a data processing and security agreement (controller to processor), upon request.
16. **Per the GDPR's definition of processing of personal data, in which countries will personal data potentially be processed?**
    - Australia, United Kingdom, United States, Canada, India, Mexico, Singapore, and Vietnam.
17. **How are Tripwire customers notified in the event of a breach or an incident?**
    - To the extent that a cybersecurity incident constitutes a legally cognizable information security breach under applicable breach notification laws, Tripwire shall notify affected organizations and individuals and relevant regulators pursuant to such laws. Definitions of a breach or an incident are defined by applicable laws.

FORTRA™

Fortra.com

About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.