PKWARE

TISAX Compliance

Meet Automotive Industry Security Standards and Build Customer Trust With PKWARE

The Trusted Information Security Assessment Exchange (TISAX) provides a framework for data security verification within the automotive industry. Through TISAX, companies undergo third-party assessments of their data security systems and processes, and share their assessment results with customers and partners.

TISAX assessments are based on requirements defined in the VDA ISA (Verband der Automobilindustrie Information Security Assessment). The assessment covers high-level corporate governance and risk management topics, as well as technical details related to data classification, encryption, and other technologies.

Automated, Data-Centric Security

PKWARE simplifies compliance with TISAX requirements, as well as GDPR and other government and industry mandates.

PKWARE's data-centric technology makes it possible to maintain control over sensitive data even in the most complex use cases. Our platform provides an array of integrated capabilities, designed for maximum flexibility and ease of use.

- Administrators use the PKWARE Enterprise Manager console to define data discovery, data classification, and data protection policies.
- PKWARE endpoint agents monitor file activity on laptops, desktops, and servers. New and modified files are scanned for data that meet's the organization's definition of sensitive information.
- Files containing sensitive data can be classified, encrypted, redacted, moved, or deleted based on company policy.
- Additional PKWARE components extend the organization's policy enforcement to mainframe and midrange systems, mobile devices, and proprietary applications.

With PKWARE, organizations can build tailored solutions to meet their unique data security and compliance goals.

PKWARE's Approach to Compliance

Data security mandates like TISAX are complex and multi-faceted, requiring the efforts of multiple departments within an organization, along with multiple vendors, partners, and advisors.

PKWARE strives to simplify compliance by providing a wide range of capabilities within a single data security platform.

Our automated, data-centric technology allows organizations to protect sensitive data on every enterprise operating system, and to create tailored workflows that meet their unique security and compliance needs.

Companies in the automotive industry can use PKWARE to meet a variety of TISAX standards, including requirements for data classification, data protection, encryption key management, and activity logging.

PKWARE's technology is also designed to fit easily into your organization's IT and security ecosystem, simplifying implementation and aiding in compliance with requirements in other functional areas such as user authentication, network security, and employee training.

MEETING VDA ISA STANDARDS FOR DATA SECURITY WITH PKWARE

VDA ISA COMPONENT	PKWARE CAPABILITIES
8.2 CLASSIFICATION OF INFORMATION **VDA ISA OBJECTIVE:** "Information shall be classified according to its value to an organization. For this classification, the value of information to the organization shall be evaluated based on factors such as confidentiality, integrity and availability. The handling of information according to its classification shall be defined and implemented by the employees."	PKWARE includes data classification in an automated workflow with data discovery and protection. • Automatically applies visual and metadata tags to files that contain sensitive information • Can be used to classify newly-created data as well as pre-existing data • Supports user-driven classification, automatic policy-based classification, or a combination of approaches
8.3 STORAGE OF INFORMATION ON MOBILE STORAGE DEVICES **VDA ISA OBJECTIVE:** "Information on mobile storage devices is generally exposed to increased risks. In order to prevent loss of information in case a mobile storage device is lost or stolen, regulations to reduce these risks shall be defined and measures shall be taken."	PKWARE applies persistent strong encryption based on an organization's data protection policies and classification scheme. • Files can be automatically encrypted using company-controlled keys • Files remain encrypted when transferred to mobile storage device or other media • If storage devices are lost or stolen, encrypted files cannot be accessed by unauthorized users
9.1 ACCESS TO NETWORKS AND NETWORK SERVICES VDA ISA requirements state that in case of high protection needs, "Data of high protection needs is to be secured at least by strong passwords, according to the state of the art." Additionally, VDA ISA requirements state that "Data of very high protection needs is to be secured by means of strong authentication (e.g. two-factor authentication).	With PKWARE, organizations can automatically detect files containing sensitive information and apply one or more remediation options: • Persistent encryption • Transparent data encryption • Quarantine • Redaction • Deletion In cases of very high protection needs, PKWARE can also require multi-factor authentication for user logins and before granting access to encrypted data.
9.5 ACCESS TO INFORMATION AND APPLICATIONS VDA ISA requirements state that "Authorization shall ensure that only authorized users have access to information and IT applications. For this purpose, access rights are allocated to the user and reviewed at regular intervals." Additionally, data requiring very high protection must be secured via "encrypted data storage in order to prevent access and viewing by unauthorized persons/roles (e.g. administrators) at least on file level."	PKWARE's management console integrates with Active Directory and applies the organization's data security policies groups and individual users, as well as devices and network locations. PKWARE offers multiple options for protecting sensitive data, including persistent data encryption and transparent data encryption. Encryption keys are associated with user identities (via Active Directory integration), so access to encrypted information can be granted and revoked by security administrators at any time.

VDA ISA COMPONENT	PKWARE CAPABILITIES
10.1 CRYPTOGRAPHY **VDA ISA OBJECTIVE:** "Protection of the confidentiality of information during both storage and transfer (e.g. when gaining physical access to data storage devices or data transfer infrastructure) shall be ensured. This is generally achieved by means of encryption. For handling encryption, it is essential that it provides the expected security characteristics at all times without simultaneously creating inadequately high availability risks."	PKWARE's technology makes it easy for employees to encrypt data no matter what operating systems or devices they use. • Key creation, exchange, and synchronization are handled in the background, leaving the encryption and decryption process transparent to end users. • Integrations with Outlook and other applications allow employees to protect sensitive information without disrupting their existing workflows. • PKWARE's management console gives security managers control over encryption keys, ensuring that the organization will always be able to decrypt its own data.
12.5 EVENT LOGGING **VDA ISA OBJECTIVE:** "Event logs support the traceability of events in case of a security incident. This requires that events which are necessary for determining the causes are recorded and stored while being protected against modification."	PKWARE's Data Security Intelligence reporting tool allows security teams and audit personnel to monitor all data discovery, classification, and protection activity. • Activity logs indicate which files are protected, where the files are stored, and which users have accessed them • Administrators can filter reporting data by time and event type, and search for specific terms within event logs • Output can be viewed directly, picked up via SIEM agent, or retrieved via API • Activity logs cannot be altered
13.4 ELECTRONIC EXCHANGE OF INFORMATION **VDA ISA OBJECTIVE:** "During exchange and transfer of information, the information security requirements shall be observed. For this purpose, it shall be defined which services within the organization may be used for which type of data and which protective measures are to be taken when using those services."	PKWARE applies persistent encryption that remains with files in transit and at rest, preventing unauthorized access no matter where the files are copied or shared. • Outlook integration secures sensitive data in message bodies and attachments without disrupting the user experience • Encryption also secures data when exchanged via cloud, FTP, and other methods
18.2 CONFIDENTIALITY AND PROTECTION OF PERSONALLY IDENTIFIABLE DATA **VDA ISA OBJECTIVE:** "Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulations, where applicable. For this purpose, processes and procedures ensuring adequate protection of personally identifiable information shall be implemented."	PKWARE technology scans files on laptops, desktops, and servers and detects personally identifiable information and other forms of sensitive data. Files containing PII can be automatically remediated based on the organization's data security policies.

PKWARE®

A global leader in enterprise data protection, PKWARE provides solutions for more than 35,000 customers around the world. Having introduced the ZIP file (the world's most widely used data compression standard) thirty years ago, PKWARE continues to innovate, helping organizations meet ever-evolving challenges in data protection and file management.

PKWARE solutions help organizations eliminate security gaps, manage sensitive data, and meet their data compliance goals. Our automated, data-centric security technology allows companies to ensure that their sensitive data is always protected according to organizational policy.

POLICY MANAGEMENT

The PKWARE Enterprise Manager allows administrators to define and apply data security policies across the entire organization.

DATA DISCOVERY

PKWARE detects sensitive data as soon as it appears on laptops, desktops, and servers, and enables automated rule-based action.

DATA CLASSIFICATION

PKWARE can apply metadata tags and visual labels to increase user compliance and facilitate policy-based remediation.

DATA PROTECTION

PKWARE secures sensitive data against unauthorized use through encryption, redaction, quarantine, or deletion.

REPORTING

Administrators can monitor activity in real time and demonstrate compliance with internal policies and external mandates.

PKWARE.com • 201 E. Pittsburgh Ave Suite 400, Milwaukee, WI 53204 • 1-866-583-1795