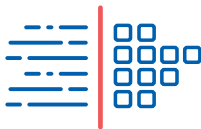


# PK Masking

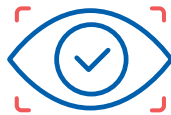
## Masking By Policy and Use Case

Fully utilized data is an enterprise's most valuable asset, but personal data without protection becomes a liability. Unstructured data is challenging to locate and protect, and companies that carry personally identifiable information (PII) and credit card data in their environments experience more frequent regulatory audits with broader scopes.

PK Masking's data protection technology can be applied at scale, masking or redacting sensitive information across petabytes of data.



DE-IDENTIFY



CONTROL



PROTECT

## Protect Privacy While Maximizing Data Value

- Allow sensitive data to be widely accessible and usable in the organization
- Optimal choice in non-production environments like dev/test, QA, or analytics
- Replace original data with realistic- or unrealistic-looking data with referential integrity
- Conceal with full or partial masking according to business needs and compliance requirements
- Protect data while migrating to the Cloud

50% of PKWARE users employ masking and redaction to protect their sensitive data



## Flexible Masking Options

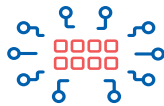
Sensitive data may reside in multiple, disparate databases across your organization. PKWARE's static masking can keep the data masked at rest while our dynamic masking only masks data when in use.

### Dynamic Masking Capabilities

- Add masking and access controls to data at the moment of query or time of access
- Cross-source data, simultaneously masking sensitive data
- Mask consistently across petabytes of cloud data stores or on premises in motion

### Static Database Masking

- Permanently obscure data with static values for entire columns
- Automatically mask sensitive data in a Database Management System (DBMS) for analytics and testing, helping organizations quickly and fully leverage the data set



Dynamic Masking  
Capabilities



Static Database  
Masking

## Extensive and Advanced Policy-Based Masking Techniques

- Consistent element-level masking
- Custom values drawn from designated expressions, tables, or functions
- Format-preservation even as values are changed
- IntelliMask with highly customized partial-field replacement value masking
- Additional options include shuffling, random, nullify, compose, XML, unstructured masking, and many more

### PK Masking helps address these compliance mandates:

- GDPR
- CCPA/CPRA
- PCI DSS
- HIPAA
- ITAR
- SOX
- TISAX
- and more...

"PKWARE provided a masking tool that was needed from security and compliance perspective. Consistent masking was one of the great features PKWARE has provided."

Senior IT Director  
Global 500 Financial Services Company

Stakeholders use PK Masking so their organizations can deserve customer trust and avoid negative consequences—with often irreversible damages—to both brand and bottom line.

## Automate Data Protection

- Automatically and permanently remove sensitive data as soon as it appears in files on computers, file servers, or in other network locations
- Secure reliable visibility into file contents to identify and redact unstructured data
- Identify and remediate valid credit card numbers while ignoring similar sequences that are not credit card numbers



PKWARE  
gives you the  
confidence  
to act on data  
in the best  
interests of your  
organization  
and the people  
who entrust you  
with their  
data.

## Intelligent Policy-Based Redaction

PKWARE's redaction solutions permanently remove sensitive information as soon as it appears in files or images.

- Match credit card-issuer algorithms for recognizing credit card numbers and automatically redact a portion of each credit card number within a file
- Render sensitive information unusable if ever the file is incidentally shared or is breached
- When an organization needs to preserve original data, a copy of the file can be created in a quarantined location prior to redaction. The unredacted version can be handed off to PK Encryption and remain compliant with applicable regulations and mandates.

**PK Protect:** Automate enterprise-wide location and monitoring of sensitive data, identity creation, data classification, and policy-based data protection techniques, ensuring complete privacy for individuals and protection of organizational personal data vulnerabilities.



PKdiscovery



PKclassification



PKmasking



PKencryption



PKprivacy

## Technical Requirements

### Technical Specifications Management Console:

- Hardware appliance
- Virtual appliance
- Software-based (Windows Server)

### Scanning and Redaction:

#### Operating Platforms

- Microsoft Windows
- macOS

#### Credit Card Number Patterns

- VISA
- MasterCard
- American Express

- Discover
- Diners
- JCB

#### File Types

- DOC/DOCX • XLS/XLSX
- PPT/PPTX
- VSD/VSDX
- XML/OOXML • PDF
- TXT
- CSV
- MDB
- ACCDB • MSG
- RTF
- LOG • JSON • Z

## Ready To See It Live? Contact Us!



[pkware.com/demo](http://pkware.com/demo)



866-583-1795



201 E. Pittsburgh Ave.  
Suite 400  
Milwaukee, WI 53204

## Follow Us



[/company/PKWARE](https://www.linkedin.com/company/PKWARE)



[facebook.com/PKWARE](https://facebook.com/PKWARE)



[@PKWARE](https://twitter.com/PKWARE)