End to End Privacy Information Compliance

An IDC InfoBrief
Sponsored by MicroFocus
Evolving IT Environments as a part of Digital Transformation

Protection of Personal Data Law (KVKK) took effect in April, 2018, with strict requirements to protect consumer data and major penalties for non-compliance.

The Protection of Personal Data Law (KVKK) came in at just the right time. Organizations now have a valid reason to redesign their data-related policies and strategies, and can undertake these activities in parallel with their digital transformation journeys.

These sectors are seeing privacy compliance as an opportunity: Oil & gas, Healthcare, Insurance, Government, Telecommunications, Other Financial Services, Utilities, Banking, Telecommunications
KVKK comes to Rescue the Data and Privacy

The deadline for conforming with KVKK was April 2018. It introduces comprehensive changes about how personal data collect, stored, analyzed and governed.

We have seen so many different types of malicious activity in the world, ranging from data leaks to the unauthorized analysis or use of personal data.

Privacy regulations are being updated globally (Asia, Latin America, Africa).

You have to hurry to eliminate your incompatibilities.

KVKK Compliance process did not end in April, just started!
If You have a business with European Citizens, Don’t Forget GDPR

The General Data Protection Regulation (GDPR) also took effect May, 2018. Contrary to what is believed, GDPR is not just for European organizations. If you employ an EU citizen or hold any data on an EU citizen, you must comply with GDPR.

According to IDC GDPR Readiness Survey results, 82% of respondents indicated that GDPR is an obstacle. Only 19% of them considered GDPR as an opportunity.

It is expected that 40% of enterprises will have failed to put adequate governance procedures and tools in place to meet the European Union's GDPR.
..Have you looked for an escape?

Fully protecting data requires different types of encryption for data at rest on storage media, data in transit over a network, and data in use on a system.

The significance of big data and analytics will show a remarkable increase.

In the end, all organizations will have to discover and classify their data as they engage in digital transformation, comply with KVKK, and identify new business models.
Do Really Know your **Environment?**

Data discovery and classification is a vital step for understanding your data. If you don’t know what data you have and where it is, you can’t comply with KVKK.

These are the key questions to ask when preparing a data inventory:

- Where is Personal Data in Databases?
- Where is Personal Data in Distributed Data Sources?
- Are we able to return within 30 days on request to the persons and institutions?
- Are we able to delete, destroy and anonymize?
- Are we able to apply the internal rules easily from one hand?
- Do we see who gets access to personal data?

Now, you have a chance to redesign your all data related process to avoid shadow IT, poor processes and hidden data flows or sources.
How Can My Organization Become Compliant with KVKK

Data Discovery
Conduct a data discovery exercise to crawl the data stores

Identification of Sources
Take an inventory of the location of the key internal and external assets

Classification
Classify data and map its location. This will help to determine where the most sensitive assets reside.

Policy Enforcement
How to move, delete, anonymize, hold the data

Governance
Review current data governance policies and update them to address workflow changes

Encryption
Facilitate risk mitigation and strengthen your data security

Data Monitoring
Identify when and where sensitive data is transmitted

Risk Assessment
Data classification and protection should be integrated into the risk assessment process for identifying vulnerable areas
KVKK suggests the use of encryption to strengthen the protection of sensitive data. The law also positions encryption as a risk mitigator factor in case of a data breach.

Format Preserving Encryption is one of the promising encryption technology which maintains the format of regulated data but replaces sensitive clear text with an irreversible hash. Using Format Preserving Encryption would facilitate your organization to encrypt sensitive data with minimum effort on all applications and databases without breaking applications or business intelligence solutions.

Choosing the right encryption method for your data is the key.

After the data discovery and classification, you have to decide which data should be considered as sensitive.

Encryption is not a one size fits all technology

Strong key management is essential! To scale and manage a robust encryption environment, the keys to unlock the data need to be managed themselves.

Encryption will make more difficult for an attacker to gain access to sensitive data.
Privacy Compliance needs a Leader..

Establish the management of your KVKK program by selecting a leader who can coordinate input from stakeholders from every part of the business and related community.

The value of data is increasing all the time. That’s why data should be secured because it offers **productivity gains and competitive advantage** but also because its access or use may cause unintended consequences such as **reputation or financial loss and regulatory compliance requirements**.

Data owners or strategists might be different units of company. According IDC EMEA GDPR research, 70% of interviewees indicated that Corporate Management or IT leads GDPR compliance process.

Source: IDC EMEA GDPR Survey, March 2017, n=560
Remember, KVKK is just Started..

Ensure that data discovery and classification processes work properly

Encrypt your sensitive data and set strong policies for encryption

Establish documentation processes

Implement control and review processes

SUCCESS
Discover and classify enterprise information
✓ Access and understand structured and unstructured data with our advanced analytics ecosystem, eliminating manual, costly, and error-prone processes, and streamlining downstream governance and migrations.

Comply with information governance mandates
✓ Meet regulatory requirements, jurisdictional retention laws, and privacy regulations with a broad compliance portfolio that has been proven in the world’s most regulated and demanding organizations.

Protect customer privacy
✓ Automate the identification of personal information (or PII) that is most important to your customers, and then secure this data throughout its lifecycle in conjunction with privacy regulations such as GDPR and KVKK.

Pseudonymization and encryption
✓ Address GDPR and KVKK guidelines for database encryption, pseudonymization, and tokenization with SecureDataHyper Format-Preserving Encryption.

Visit www.microfocus.com to learn more.