

Meeting Key GDPR Requirements with Encryption & Trust Management



The GDPR Requires Stronger Data Protection

Protecting private data will be more critical than ever

- New restrictions around the collection, retention and disclosure of personal data
- More scrutiny of the users and applications that have access to private data

Substantial penalties

- Orgs found in violation face penalties up to €20 million or 4% of annual worldwide revenues



Addressing the GDPR with Encryption & Trust Management

Data encryption

- Organisations “shall implement appropriate...measures” including “encryption of personal data”. (*Article 32*)
- In the event of a data breach, the organisation is exempt from notifying customers if it had in place measures that “render the personal data unintelligible...such as encryption.” (*Article 34*)

Trust management

- Organisations are required to “protect against unauthorised or unlawful processing...using appropriate technical or organisational measures ('integrity and confidentiality')." (*Article 5*)

Thales Solutions Address Key GDPR Requirements

■ Data encryption

- File, database and application-level encryption for data at rest
- Network encryption for data in motion

■ Trust & Identity management

- Privileged user access management and strong authentication ensure that only authorized users and devices can access personal data

■ Underpinned by strong key protection & management

- Encryption key protection based on industry best practices

Thales Solutions Address Key GDPR Requirements

Data encryption

- File, database and application-level encryption for data at rest
- Network encryption for data in motion



Vormetric Data Security Platform

- Data-at-rest encryption based on your business requirements
- File-level, application-layer, transparent encryption



Datacryptor 5000 Series

- Encryption of data in motion



Thales Solutions Address Key GDPR Requirements

■ Data encryption

- File, database and application-level encryption for data at rest
- Network encryption for data in motion

■ Trust & Identity management

- Privileged user access management and strong authentication ensure that only authorized users and devices can access personal data

■ Underpinned by strong key protection & management

- Encryption key protection based on industry best practices

Thales Solutions Address Key GDPR Requirements

Trust & Identity management

- Privileged user access management and strong authentication ensure that only authorized users and devices can access personal data

THALES

nShield HSMs

- Strong, cryptographically-based authentication of users and devices



Vormetric Data Security Platform

- Privileged user access management



Thales Solutions Address Key GDPR Requirements

■ Data encryption

- File, database and application-level encryption for data at rest
- Network encryption for data in motion

■ Trust & Identity management

- Privileged user access management and strong authentication ensure that only authorized users and devices can access personal data

■ Underpinned by strong key protection & management

- Encryption key protection based on industry best practices

Thales Solutions Address Key GDPR Requirements

Underpinned by strong key protection & management

➤ Encryption key protection based on industry best practices

THALES

nShield HSMs

- FIPS-certified security
- Tamper-resistant hardware
- Automated key lifecycle & replacement

Vormetric
A Thales company

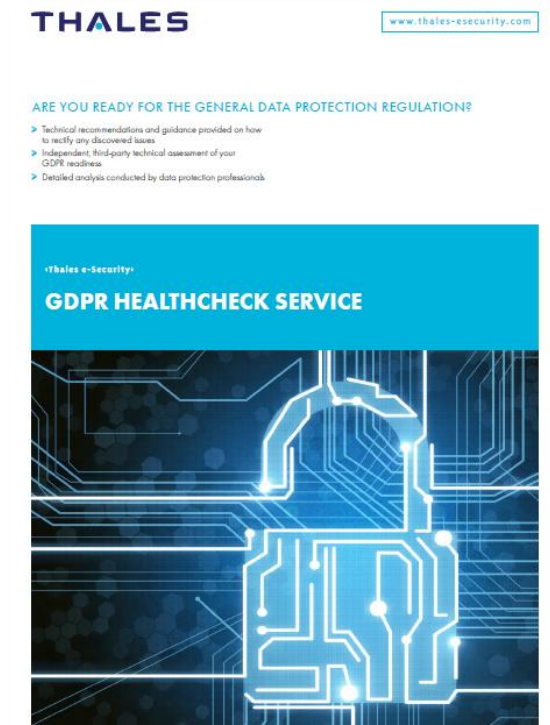
Vormetric Data Security Manager

- Centralized management of encryption keys and policies
- Consolidated key management for Oracle and Microsoft SQL Server



GDPR Healthcheck Service

- Independent, third-party technical assessment of your GDPR readiness
- Technical recommendations and guidance on how to rectify any discovered issues
- Detailed analysis conducted by data protection professionals
- Presentation of findings to key stakeholders



Meeting Key GDPR Requirements with Encryption & Trust Management

