THALES
Building a future we can all trust

Digital Sovereignty through Secure Key management

Kaare.mortensen@thalesgroup.com
www.thalesgroup.com

Sovereignty

Supreme authority in a state

subject to the recognized limitations imposed by international law.

The Oxford Reference

Digital Sovereignty = Control

"**Digital sovereignty** refers to the ability to **control** your own digital destiny – the data, hardware, and software that you rely on and create."

World Economic Forum

Digital Sovereignty & Cloud Adoption

Cloud = somebody else's computer

- User needs control = Digital Sovereignty

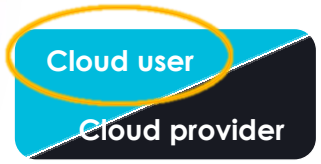
Impacts of Cloud Adoption

- Loss of direct control (outsourcing)
- Multinational law enforcement

Loss of direct control

Users' Responsibilities in the Cloud:

- Security IN the Cloud
- Data Protection and Access Controls



Cloud Shared Responsibility

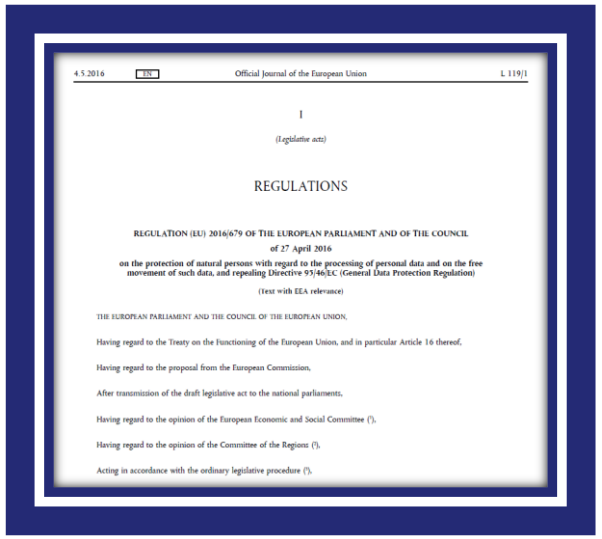
	Private	IaaS	CaaS	FaaS	SaaS
Operational resilience					
Identity and Access Mgt					
Data					
Application					
Runtime					
OS, K8's, Services					
Virtualisation					
Infrastructure (DC, Networking, Storage, Compute)					

Multinational law enforcement

Apple Threatens to Pull FaceTime and iMessage in the UK Over Proposed Surveillance Law Changes

- the Online Safety Bill requires companies to install technology to scan for child sex exploitation and abuse (CSEA) material and terrorism content in encrypted messaging apps and other services.

Regulation EU GDPR


4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL
of 27 April 2016
on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)
(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee (1),

Having regard to the opinion of the Committee of the Regions (2),

Acting in accordance with the ordinary legislative procedure (3),

Organisations "shall implement appropriate **technical and organisational measures** including **encryption of personal data**;"

GDPR, Article 32

Personal data is protected by the "use of additional information **[Keys], kept separately** and subject to technical and organisational measures"

GDPR, Article 4

Source:
EU GDPR General Data Protection Regulation

GDPR & extraterritorial transfers (“Schrems2”)

Technical Measure + Organisational Measure

“the personal data is processed using strong **encryption**”
“the **keys are reliably managed** (generated, administered, stored, if relevant, linked to the identity of an intended recipient, and revoked)”
“the keys are retained solely **under the control of the data exporter**”

EDPB post-Schrems2 recommendations

Regulation EU GDPR

noyb

New Trans-Atlantic Data Privacy Framework largely a copy of "Privacy Shield". *noyb* will challenge the decision.

The fundamental problem with FISA 702 was not addressed by the US, as the US still takes the view that only US persons are worthy of constitutional rights.

Source:
EU GDPR General Data Protection Regulation

NIS2 (Network and Information Security)

BRIEFING

EU Legislation in Progress

European Parliament

The NIS2 Directive

A high common level of cybersecurity in the EU

OVERVIEW

The Network and Information Security (NIS) Directive is the first piece of EU-wide legislation on cybersecurity, and its specific aim was to achieve a high common level of cybersecurity across the Member States. While it increased the Member States' cybersecurity capabilities, its implementation proved difficult, resulting in fragmentation at different levels across the internal market.

To respond to the growing threats posed with digitalisation and the surge in cyber-attacks, the Commission has submitted a proposal to replace the NIS Directive and thereby strengthen the security requirements, address the security of supply chains, streamline reporting obligations, and introduce more stringent supervisory measures and stricter enforcement requirements, including harmonised sanctions across the EU. The proposed expansion of the scope covered by the NIS2, by effectively obliging more entities and sectors to take measures, would assist in increasing the level of cybersecurity in Europe in the longer term.

Within the European Parliament, the file has been assigned to the Committee on Industry, Research and Energy. The committee adopted its report on 28 October 2021, as well as a mandate to enter into interinstitutional negotiations.

"essential and important entities shall take appropriate and proportionate **technical and organisational measures**, include at least:

- policies on risk analysis and information system security;
- **supply chain security**;
- the use of **cryptography** and **encryption**"

NIS2, Article 21

Digital sovereignty and AI –can you prove it?

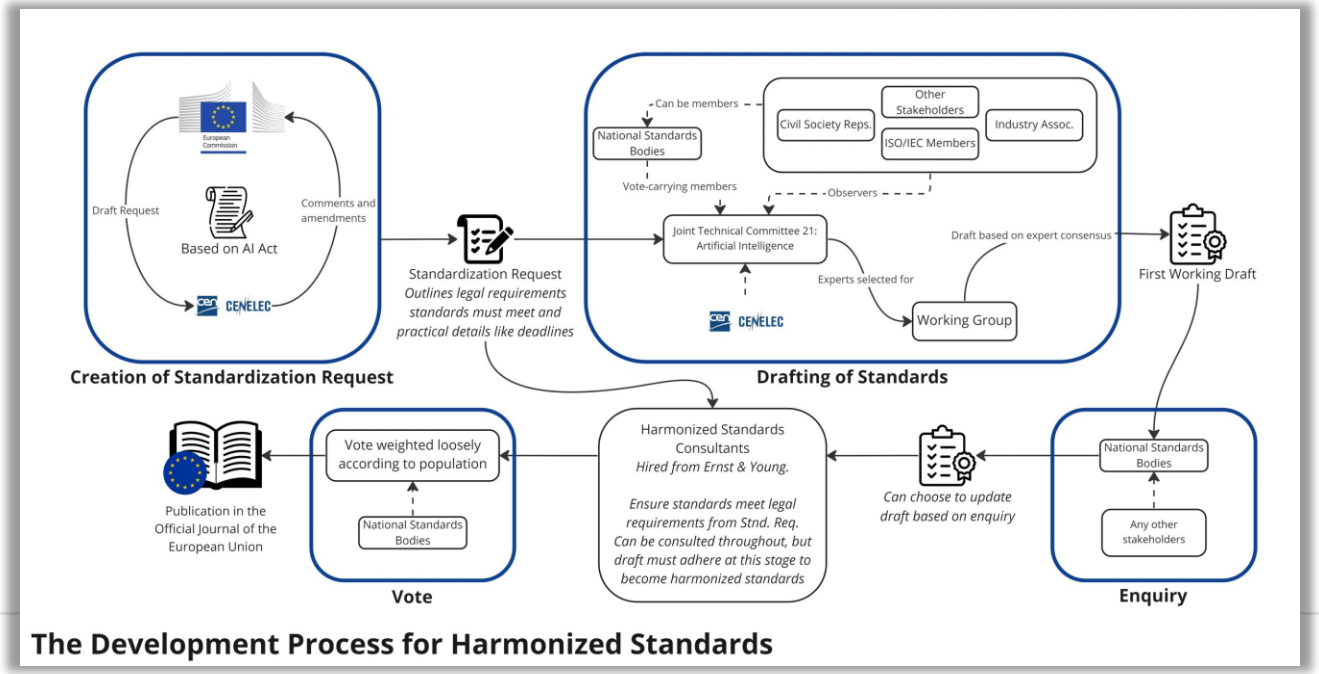
Source: www.9news.com.au

The AI Act

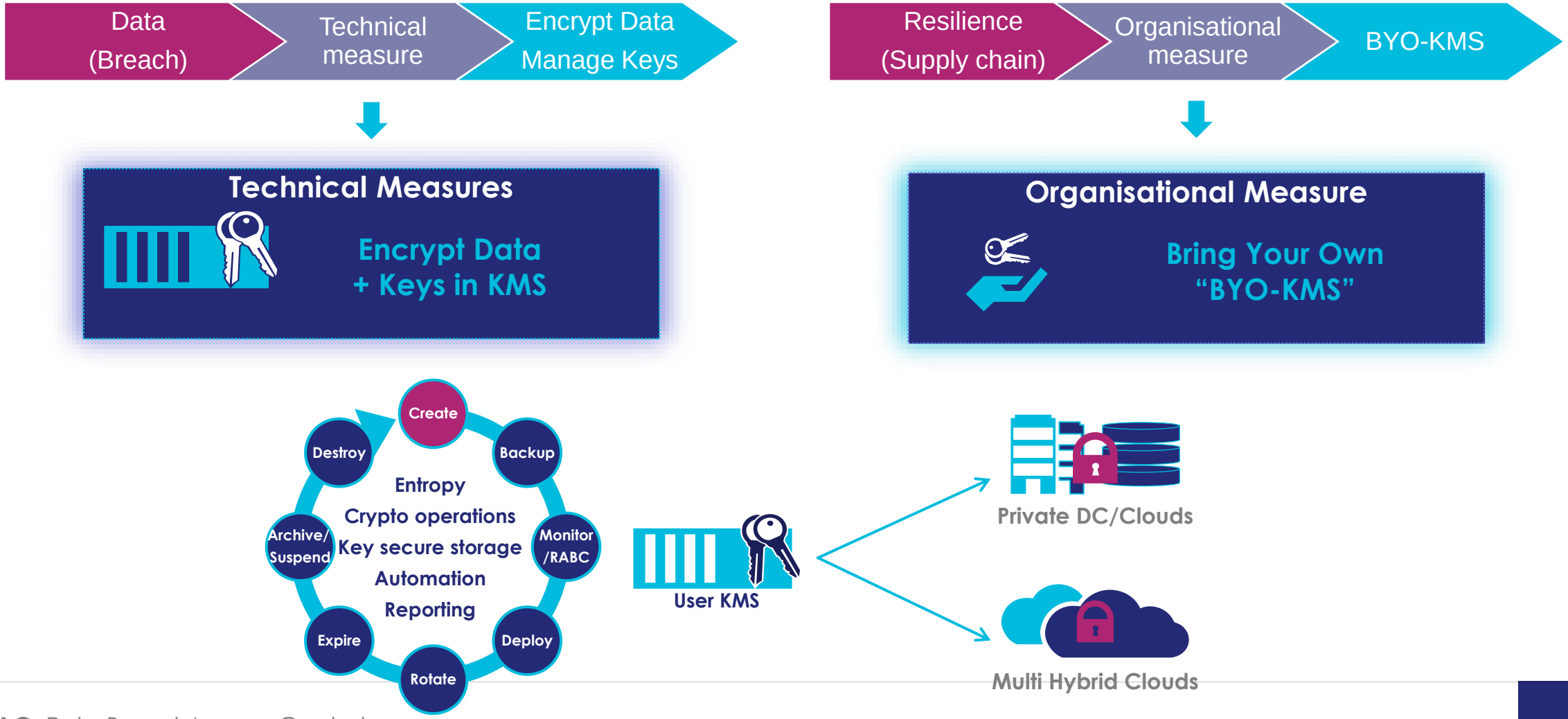
EUROPEAN COMMISSION

The AI Act is a proposed European law on artificial intelligence (AI) the first law on AI by a major regulator anywhere.

- Ensure that AI systems placed on the Union market and used are safe and respect existing law on fundamental rights and Union values
- Early 2025: Finalise standards, to be in place before AI Act is applied.



User-controlled encryption and cloud key management
= sovereignty-enhancing technology



RBAC: Role-Based Access Control
KMS: Key Management System

The Big Picture

CipherTrust Connectors

Discovery and Classification

Ransomware Protection, Encryption and Access Control

Database Protection

Application Data Protection

Tokenization

Secrets Management

CipherTrust Cloud Key Manager

ORACLE CLOUD

Microsoft Azure

salesforce

Google Cloud Platform

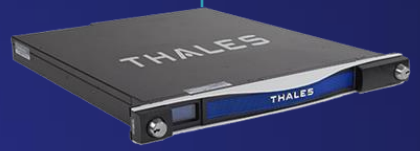
SAP Cloud Platform

amazon web services

CipherTrust Manager

Enterprise Key Management and Policies

High Speed Network Encryptors



Luna HSM

Root of Trust

Enterprise Key Management

For native encryption

Oracle
MySQL
MS Always Encrypted
IBM DB2

Powered By vmware vSAN

vSAN/vCenter
Hadoop
Custom Apps

Full Disk Encryption
Tape Archives
NTAP, Pure, EMC, IBM, Hitachi, Dell, etc.

THALES
Building a future we can all trust

THALES
Building a future we can all trust

Thank you

www.thalesgroup.com