



CanaryBit

Born in Sweden • Made for Europe



Scalable Compliance by Design

Security Automation with
Trusted Execution Environments

NICOLAE PALADI, PhD

CEO & Co-founder

nicolae@canarybit.eu



The Gap That Compliance-by-Design Cannot Ignore



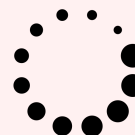
AT REST

ENCRYPTED



IN TRANSIT

ENCRYPTED



IN USE



NOT ENCRYPTED

CONFIDENTIAL COMPUTING

**Trusted Execution
Environments (TEE)**

Remote Attestation

Runtime confidentiality and integrity of data and workloads

END-TO-END DATA PROTECTION



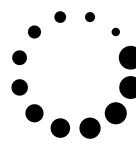
AT REST

ENCRYPTED



IN TRANSIT

ENCRYPTED



IN USE

ENCRYPTED

"Protection of data in use remains a central and complex area of modern information security."

Swedish Data Protection Authority (IMY) · Report IMY-2026-5444 · March 2026

USE CASE: PROCESSING PERSONAL DATA FROM VEHICLE SENSORS

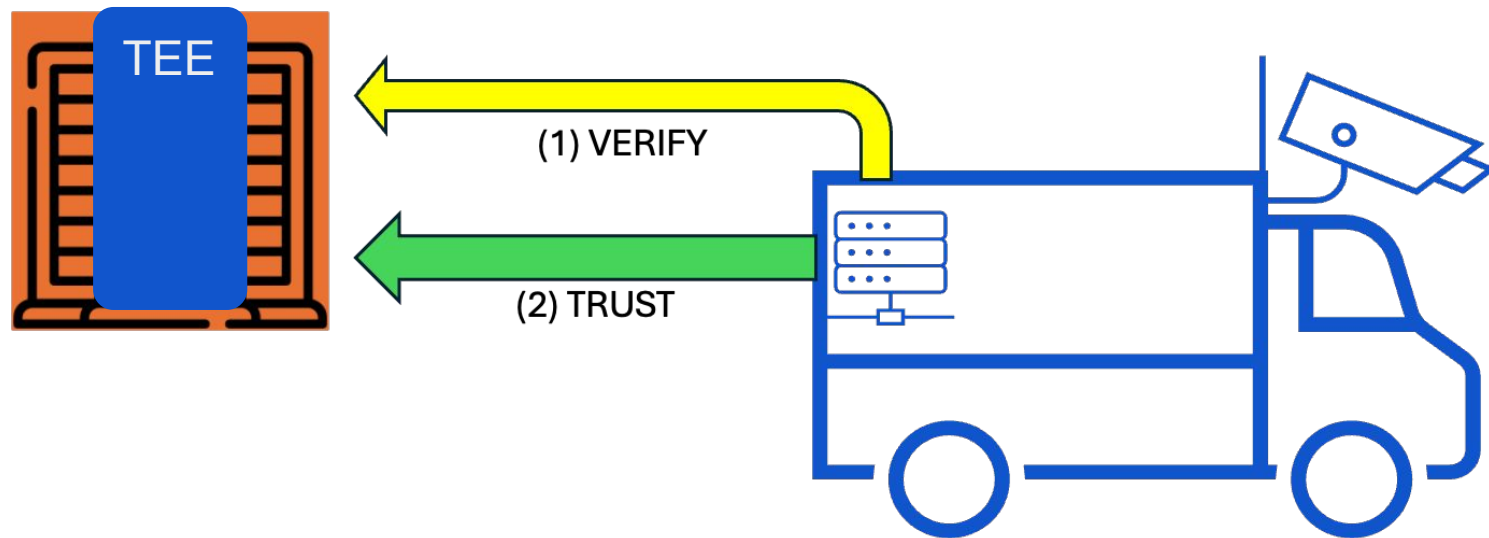
Data processor



Data controller



USE CASE: PROCESSING PERSONAL DATA FROM VEHICLE SENSORS



Claim third party cloud $\neq$ data processor tested with Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten)

IMY REGULATORY SANDBOX RESULTS



PARTICIPANTS

- IMY - Data Protection Authority
- Volvo Group
- Ericsson
- Canary Bit



Report
IMY-2026-5444



SUBJECT

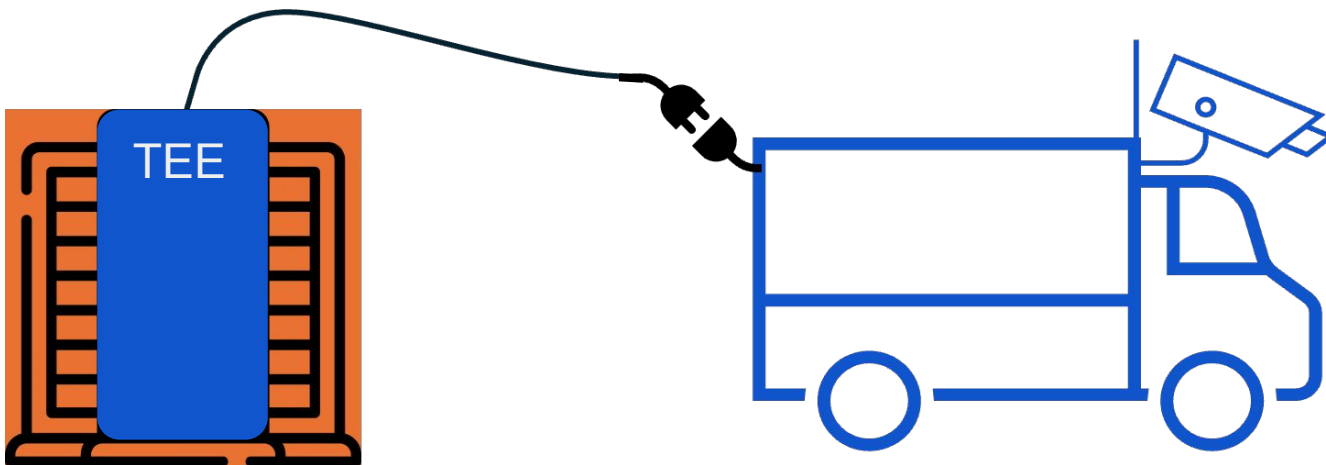
- TEE deployment on AMD SEV-SNP & Intel TDX
- Independent remote attestation (**not** provider-controlled)
- Confidential AI on NVIDIA H100
- GDPR compliance of the confidential compute model



OUTCOME

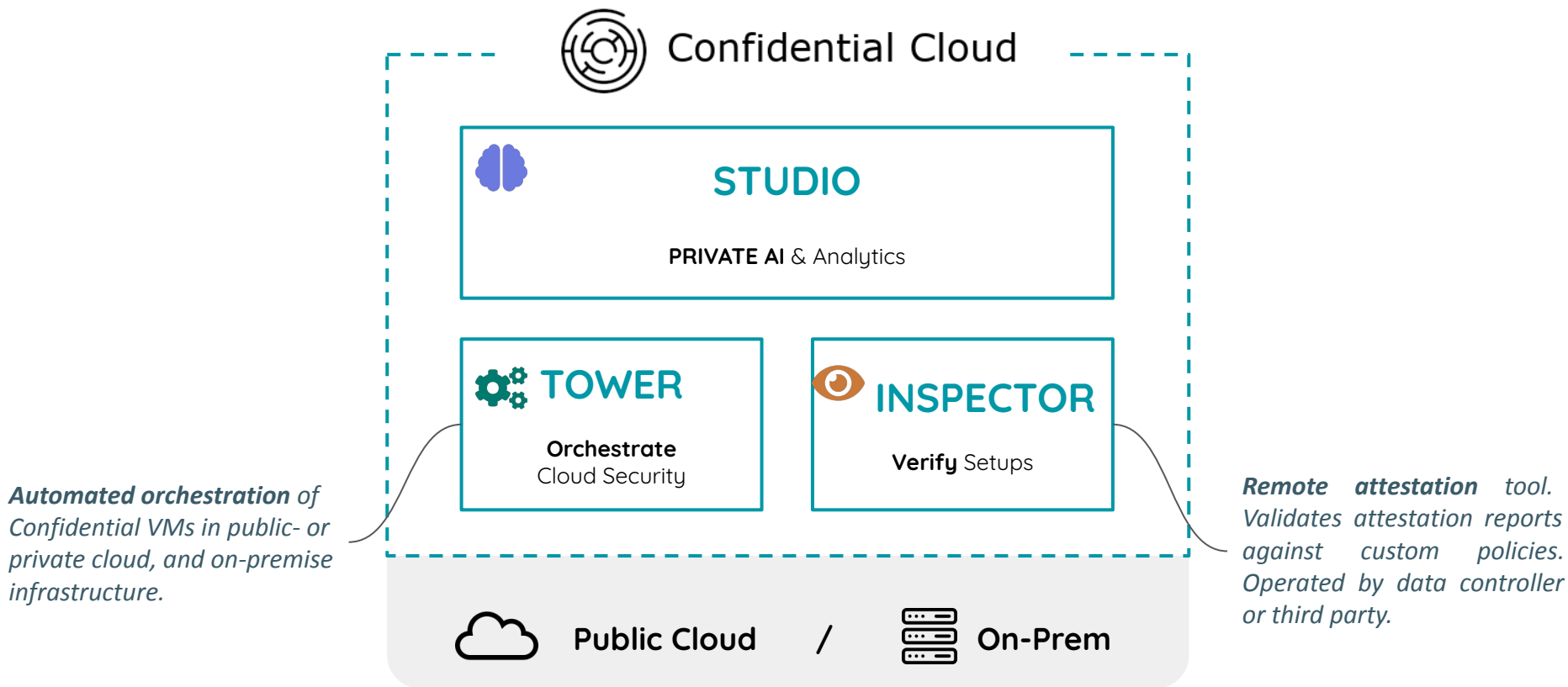
- **GDPR Art. 25 - data protection by design**
- **GDPR Art. 32 - appropriate technical measures**
- **Infrastructure provider not data processor**
- Legal linchpin: Independent verification mechanism
- Data controller **must** hold the verification mechanism

IMY REGULATORY SANDBOX MAIN TAKEAWAYS



- (1) Infrastructure provider not a data processor if TEE attested by data controller.
- (2) Data controller must hold the verification mechanism

THE PLATFORM



FURTHER DEPLOYMENT EXAMPLES



Mission-Critical Infrastructure

- Sensor data from restricted facility processed in TEEs to limit exposure and ensure verifiable traceability
- Demonstrator TRL 7



Healthcare Data

- Privacy-preserving cross-border analysis of sleep disfunction data using TEEs
- Contribution towards EOSC
- Aligned with Secure Processing Environments for EHDS (DIGG 2026-00634)



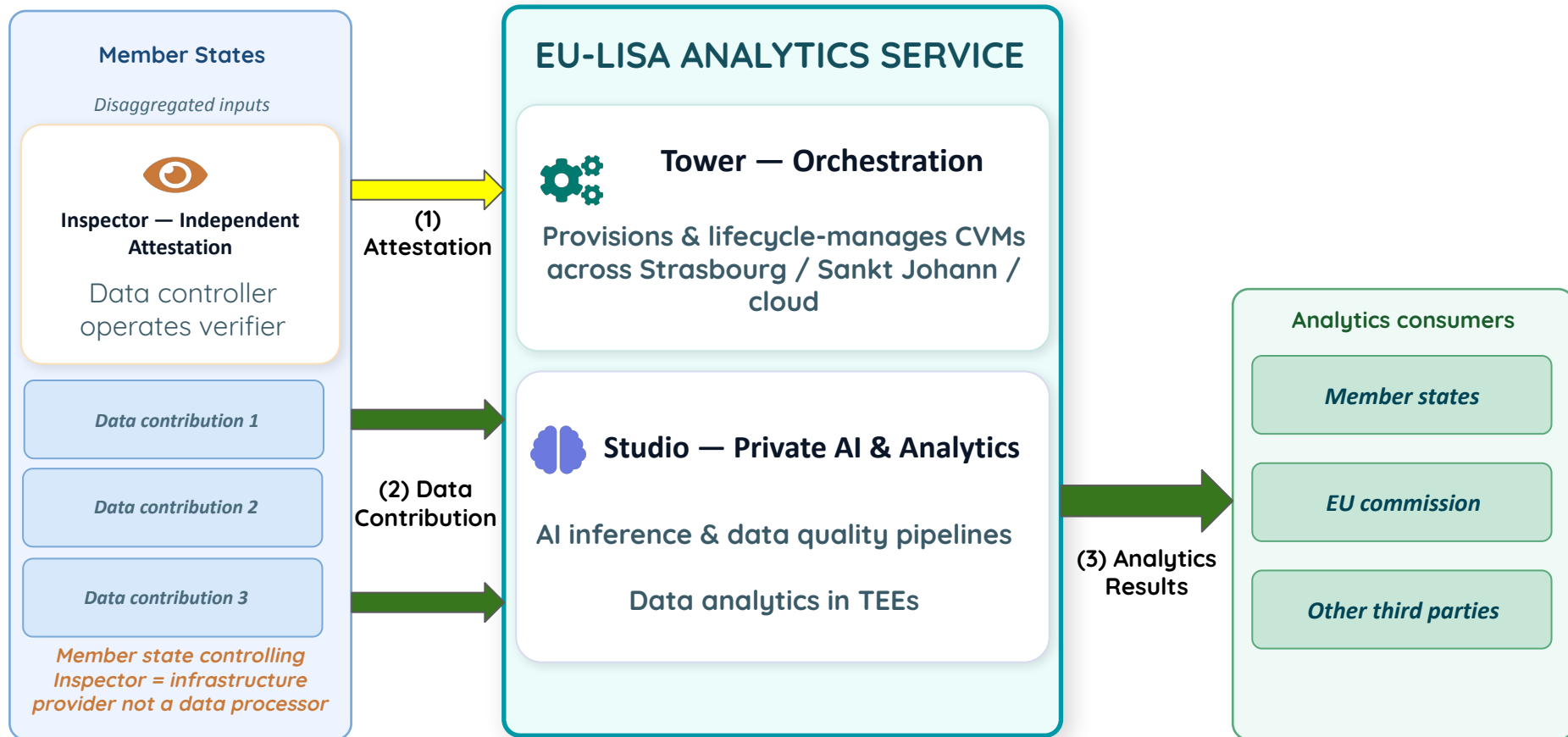
Cyber Threat Intelligence

- Privacy-preserving cross-border CTI sharing.
- Regional authorities in ES, IT
- Included in report on use of PETs for efficient public administration (Fi 2025:07)
- Demonstrator TRL 8

“Use of confidential computing will increase in public administration.”

Swedish Ministry of Finance · Privacy Enhancing Technologies in Public Administration, SOU2026:44 · July 2026

EU-LISA EXAMPLE: PRIVATE ANALYTICS ON SENSITIVE DATA



TAKEAWAYS

Security automation enables data protection and compliance at scale.

Infrastructure provider not a *data processor* if TEEs attested by data controller.

Use of TEEs can satisfy GDPR Art. 25 and Art.32 **by design**.



NICOLAE PALADI, PhD
CEO & Co-founder
nicolae@canarybit.eu

Contact me!

