Manufacturing European Software

Your software is now a (European) product.

Daniel Thompson-Yvetot - July 2, 2025. GC25

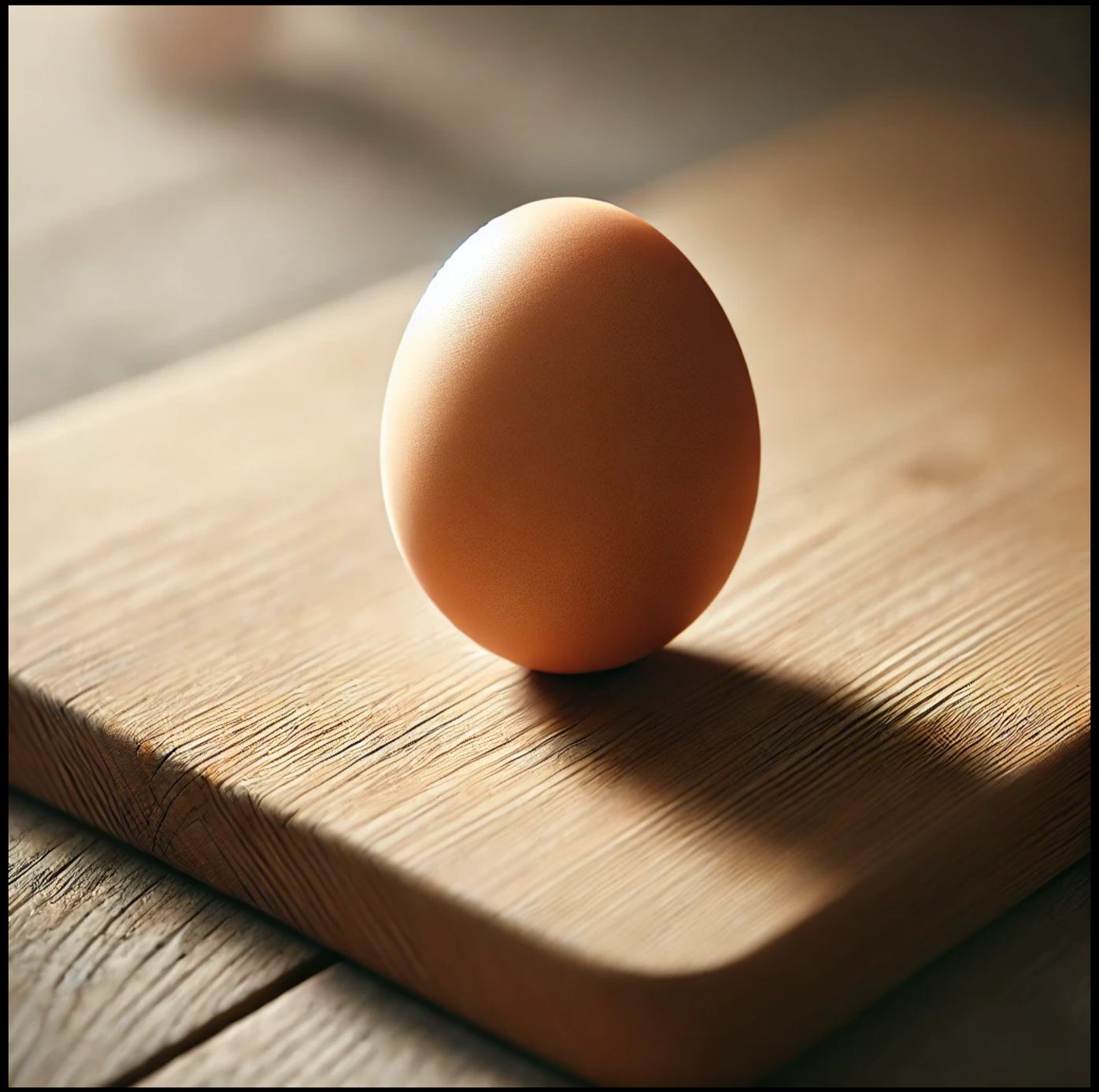
DIF / EF / Tauri / CrabNebula

Daniel Thompson-Yvetot

Tauri Founder
CrabNebula CEO
Open Regulatory Compliance Working Group Member
ETSI Rapporteur for CRA Vertical Standards
Product Guy, Entrepreneur, Author, Speaker
Dad, Woodworker, Photographer, Friend
Thinks Polyform Noncommercial is sometimes better than OSS

PDE from the CRA

> **All products** with digital elements that have an intended and foreseeable use that includes direct or indirect data connection to a device or network will have cybersecurity obligations imposed upon them.



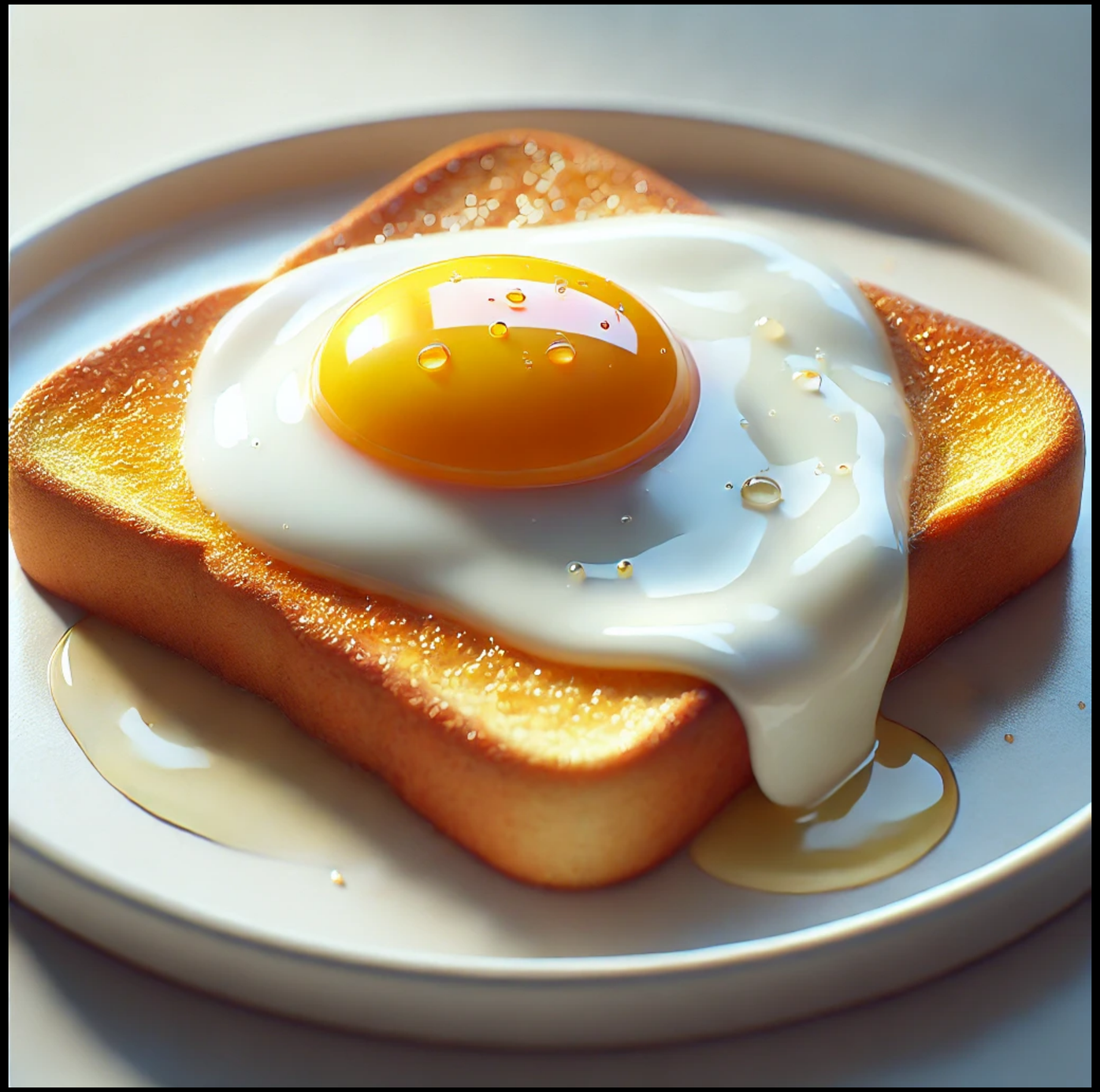
A component
is a product.

Products can be dangerous.

https://www.researchgate.net/figure/Microscopic-View-of-Salmonella_fig1_282879768

So regulators mount up.

https://willita.en.made-in-china.com/product/MnKRfoiyLvWd/China-Egg-Stamping-Code-Machine-Coding-Printer-Egg-Printing-Machine.html



Because consumers deserve safety

But products
can get complicated

The NLF

The NLF

- New Legislative Framework
- Comprehensive regulatory overhaul (2008)
- Enhanced market surveillance
- Improved accreditation system
- Clearer obligations for economic operators
- Reinforced CE marking credibility

The Blue Guide

The Blue Guide

- Single Market Business Rules
- Descriptive, not prescriptive
- Definitions of market players
- Defines what constitutes a product

Standards

Standards

- Horizontal
- Vertical
- Presumption of Conformity
- Never required

Products with Digital Elements

Products with Digital Elements

A software or hardware product and its remote data processing solutions, including software or hardware components being placed on the market separately.

Cyber Resilience Act

Cyber Resilience Act

- **In Force** Dec 2024
- In partial application (reporting) Sep 2026
- **In Application** Dec 2027
- Partial retroactive compliance
- Components are products
- Fines according to revenue of company
- Ability to remove market access

Cyber Resilience Act

- Declaration of Conformity
- User Manual
- SBOM
- Cybersecurity risk assessment
- Reporting
- 5 years of maintenance
- 10 years of records keeping

Cyber Resilience Act

- Default => Most software / libraries
- Important II, Critical => require CAB assessment
- Non-European companies need EU Auth. Rep
- Change of risk => new declaration of conformity

Product Liability Directive

Product Liability Directive

- Only for non-business use by natural persons
- Open Source components not considered
- Joint and several liability
- No-fault liability
- 10 years of records keeping
- Maybe* safe if CRA compliant

Product Liability Directive

- New classes of liability
- Psychological Damage
- Data loss

Open Source Software Stewards

Open Source Software Stewards

- Foundations, non-profits, some companies
- Not considered manufacturers, because they are not participating in market activity
- No CE Marking
- Cybersecurity reporting
- Expectation of “no associated market activity”

Diligent Product Planning

Diligent Product Planning

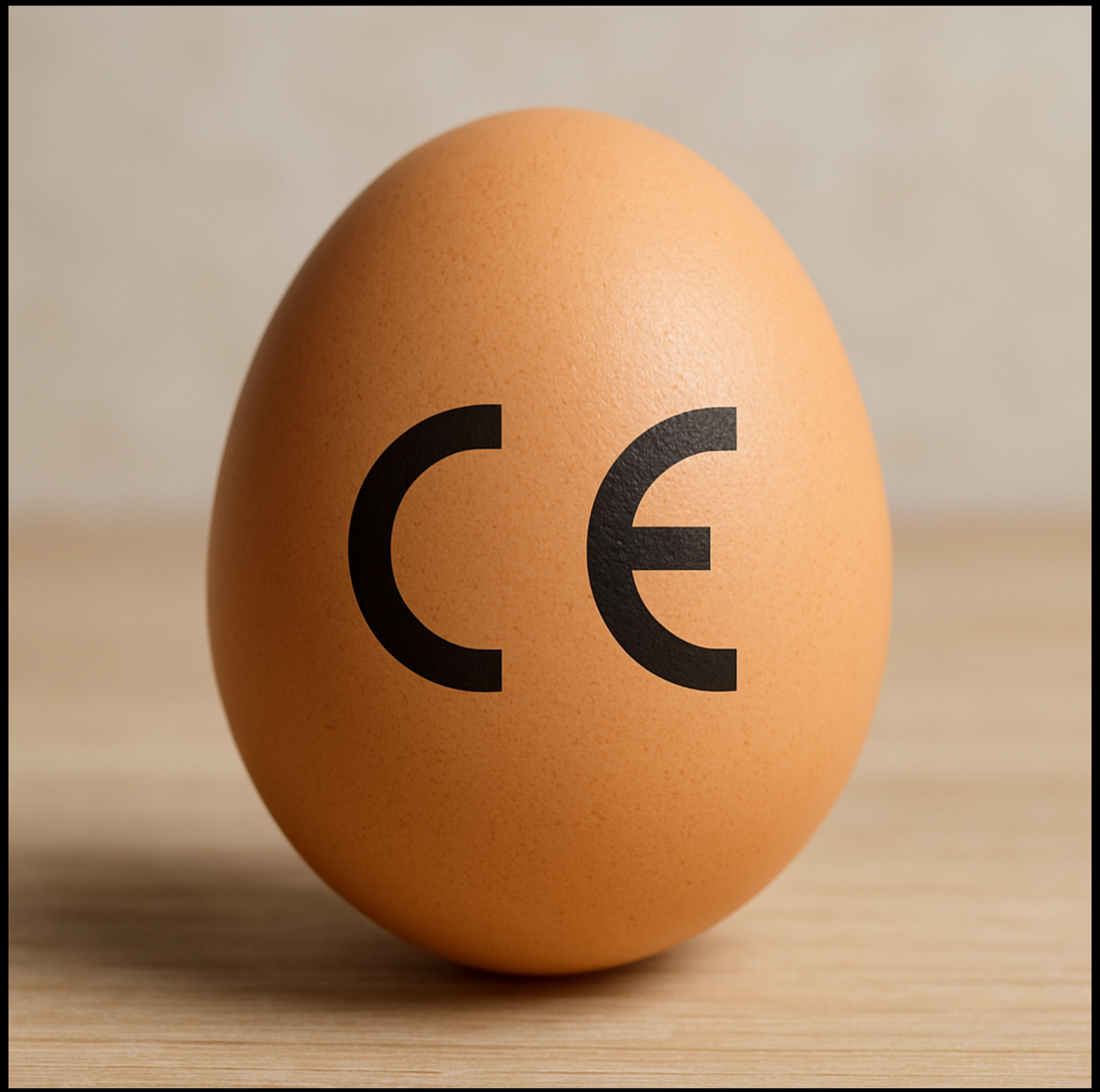
- Include security assessment early
- Consult with compliance team
- Plan all features at beginning
- Maintenance mode needs engineers
- Don’t charge for your Beta

If you only remember one thing from this entire talk:

The European Regulatory Banhammer

will remove your product
from the market
if it does not comply.

So, declare your conformity:


CE

I wrote THE book about this topic, for product people: