



Falsehoods FOSDEM attendees believe about the CRA

**as overheard by a technologist (not a lawyer!) whose job it is to
know the CRA**

aka let's speed run an FAQ

I work on Cyber Resilience Act standards
and read it all the time

skipping the rest of an intro,
I only have 256 seconds

Co-funded by



Co-funded by
the European Union

On typical open source projects

Falsehood 



I'll have to pay a big fine if my
open source project has a
vulnerability

Falsehood 



Co-funded by
the European Union

**Donations or sponsorships for my
work in Open Source makes me
personally liable**

Falsehood 



Co-funded by
the European Union

My work on an open source
project could make my employer
liable for it

Falsehood 

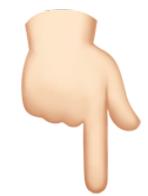


**Releasing an open source project
means I have to do compliance
documents if anyone integrates it**

Falsehood 



I have to find an “open source steward” for my project

Falsehood 



Co-funded by
the European Union

I'll just be an “open source
steward”

Falsehood 



Co-funded by
the European Union

The CRA requires projects to
follow specific processes

Co-funded by



Co-funded by
the European Union

On products, doing business

Falsehood 



Any CVE on my integrated components will set me up for a big fine

Falsehood 



Co-funded by
the European Union

As long as it's not for sale with a
price tag, it's not a “product”

Falsehood 



**Integrating a CE-marked
component covers my “due
diligence” requirements**

Falsehood 



Commercial products won't want
to integrate open source anymore

Falsehood 



Co-funded by
the European Union

Any update to a product means I
have to do a complicated
assessment all over again

Co-funded by



Co-funded by
the European Union

Bonus round

Falsehood 



Co-funded by
the European Union

RCAAs must be released within 24 hours of discovering a vulnerability

Falsehood 



The ecosystem will be full of
“CRA Compliant” forks