Due Diligence
Due Care
Reasonable Person

Due Diligence & Vulnerability Handling Task Force

2026-05-07

Salve J. Nilsen <sjn@cpansec.org>

IANAL

- Personal understanding
  - (…though checked with Brussels-based lawyer)

- Please check with your own lawyer

No clear definitions

- On purpose
- Clear definitons may help some, but restrict others
- Clear definitions invite exploitation and loop-holes

- Also: No harmonized understanding on EU level
  - This is left to general principles in civil law
- Also: CRA’s delegated acts may say something?
  - Unlikely to go against common practice
- Also: Civil liability laws matter
  - Directive 2024/2853 on liability for defective products

Due Diligence: Unlikely to be well-defined

- Instead – ask “What constitutes negligent behavior?”
  - Answer: “It depends!”

“Reasonable Person”

- “What would a reasonable and prudent person do under similar circumstances?”
  - A hypothetical person
  - Circumstances, level of control, competence, difficulty of the task, best practices in the field, etc.
- “Reasonable professional”
  - Cannot hide behind ignorance
  - A specialist is expected to not do "rookie" mistakes

“Due Care”

- A standard of behaviour
- An outcome - to act responsibly
- To do this, you must *do your due diligence*

What may “Due Diligence” in CRA mean?

- Do the expected preparations and work a *Reasonable Professional* would do, so they may act with *Due Care*

- Reasonable Security Professional
- Reasonable Business Continuity Officer
- Reasonable Software Developer
- Reasonable Open Source Contributor

What would a Reasonable Professional do?

Open Source-compentent Security Professional

- For each relevant component in the dependecy graph,
  Ensure and Verify…
  - …relevant development practices are followed
  - **…**all relevant components are taken care of in a responsible manner, and live up to relevant expectations
  - **…**you have ways to discover relevant issues
  - **…**you can respond to and mitigate relevant issues in a timely manner
  - **…**policies exist and adhered to
- etc.

Thanks!

- Questions & comments

Salve J. Nilsen <sjn@cpansec.org>