Helpful replies for FOSS developers

(Not legal advice)

- **Q: We are a manufacturer performing due diligence for open source code contained in our product. You must give us a software bill of materials (SBOM) for your code!**
  A: As a non-commercial FOSS developer, I have no obligations under the CRA. See CRA Article 2(1) and CRA Recital 18.
- **Q: We are a manufacturer affected by a security bug in your FOSS code contained in our product. Fix it now!**
  A: As the upstream non-commercial FOSS developer, I have no obligations under the CRA. See CRA Article 2(1) and CRA Recital 18. Oh btw, if you develop a fix you have to share it with me for free. See CRA Article 13(6) and Recital 34.
- **Q: We as a manufacturer of a PwDE containing your FOSS code will not tell you about security bugs in your FOSS project unless you sign an NDA.**
  A: You are legally required by the CRA to report the vulnerability to me, no NDA required. See CRA Article 13(6) and Recital 34.
- **Q: Do some bugfix/SBOM declaration/feature for CRA standards compliance for us for free!**
  A: Haha no. I‘m a non-commercial FOSS dev, zero CRA obligations. If you want me to do that, you can pay me for my time+resources.