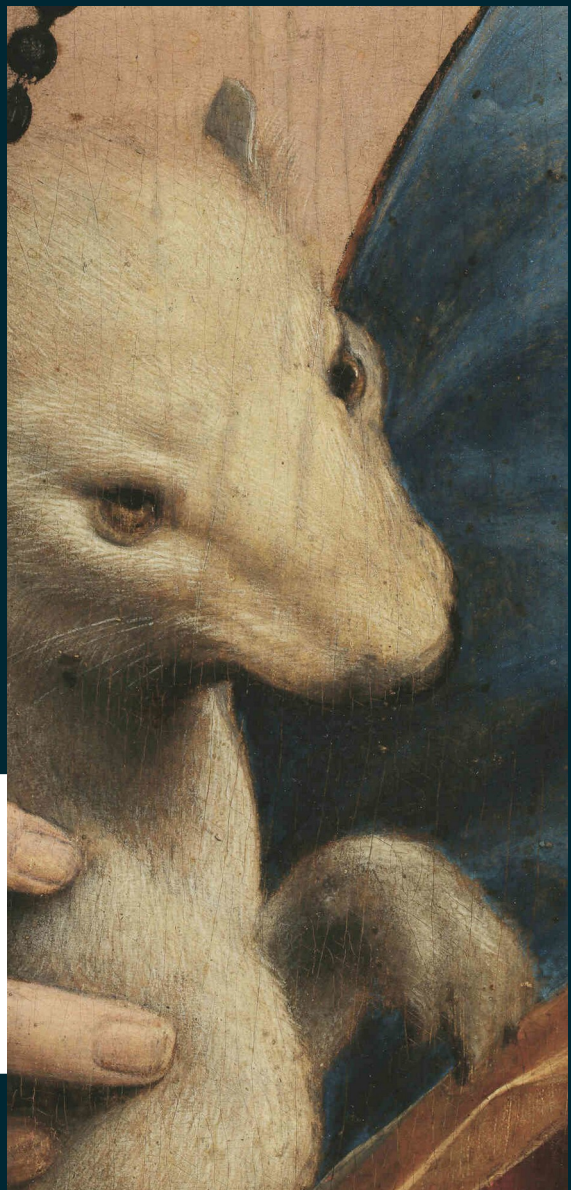
The Hermine Project

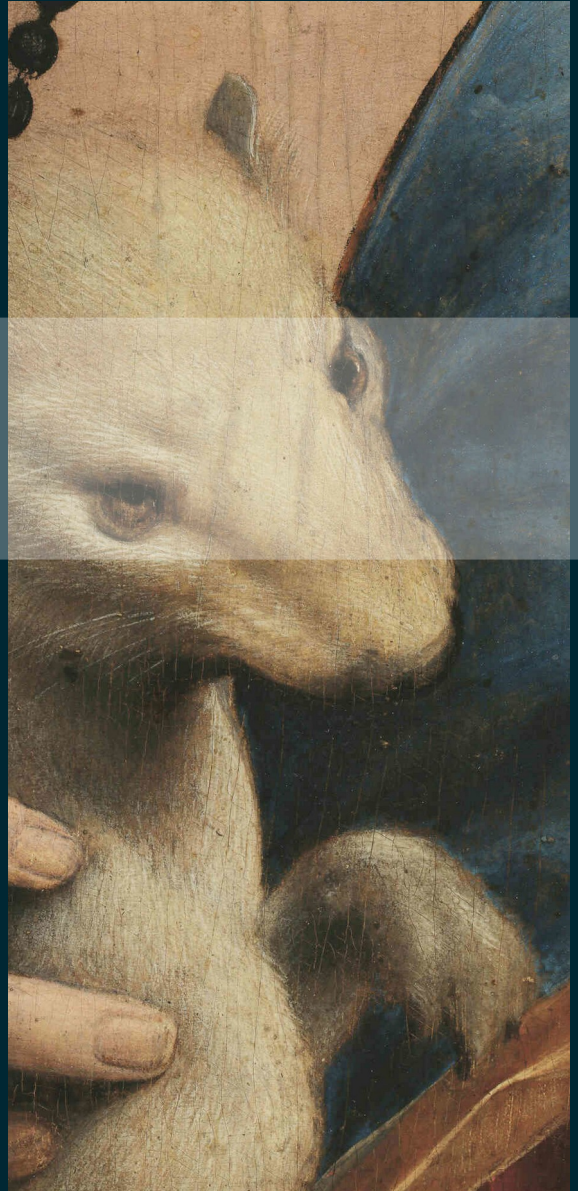
Automate legal compliance with Hermine



June 15th, 2023

Benjamin Jean, Céline Fontaine,
Maxime Rolland et Thibault Millien

Who we are



A FOSS, community driven project

The Hermine project has been started 18 month ago by 6 end-user & partner companies.

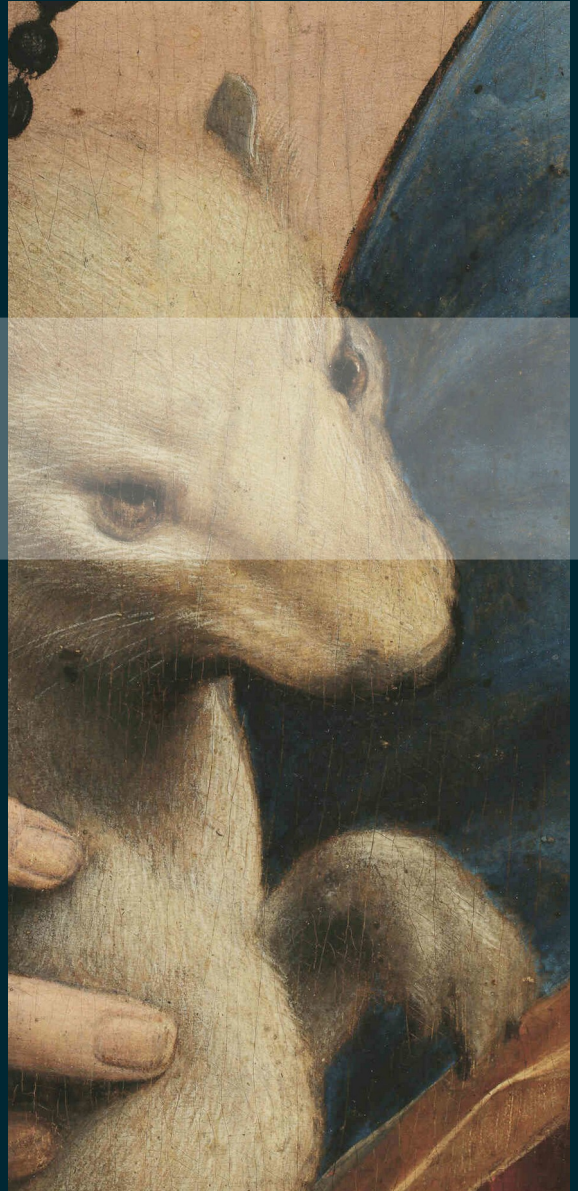
- No dedicated organisation yet (3 committees : legal, technical, steering)
- As open as possible (and as closed as necessary):
  - Licences : Code (AGPL-3.0-only) & Data (OdbL-1.0)
  - No CLA, just a DCO
  - Code of conduct : Contributor Covenant, version 2.1

The general spirit towards compliance

Hermine aims at being **efficient and pragmatic** while **limiting legal uncertainty.** We rely on a collective & shared approach to compliance (standardizing legal -- peer-reviewed -- understanding of main licences).

Compliance tool. By being highly configurable, Hermine fits specific open source policies (allowing each organisation to decide on the level of risk it considers acceptable).

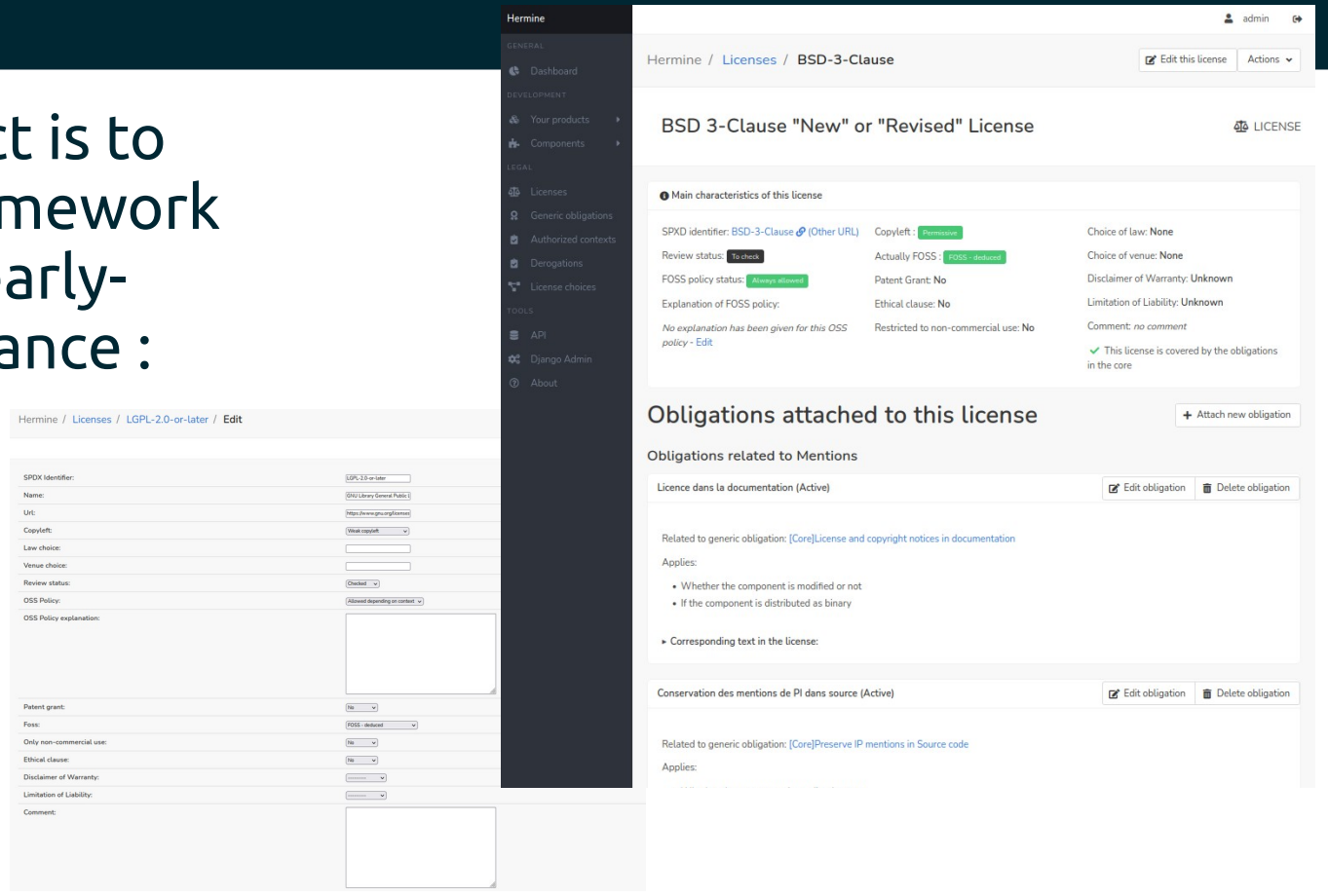
Demonstration



We analyse licences

One goal of the project is to provide a systemic framework to analyse FOSS (or nearly-FOSS) licences, to instance :

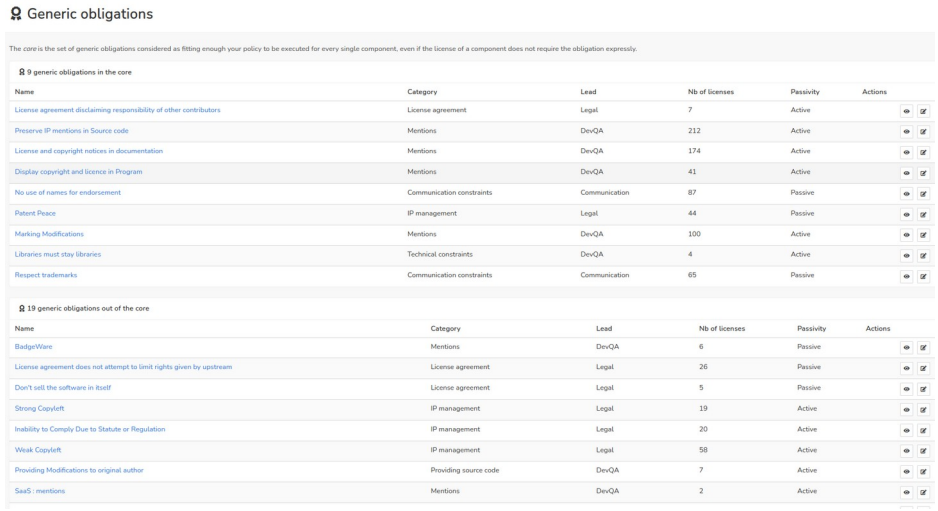
1) LGPL-2.0-or-later
2) BSD 3-Clause



https://hermine-foss.org/

We define a core set of generic obligations

- We breakdown every licence in a set of obligations, mentioning for each how it is triggered.
- If the meaning of the obligation is very common (e.g. there is more than 200 ways to say “copy the licence in the documentation”), we link it to **a generic obligation.**



Generic obligations

The *core* is the set of generic obligations considered as fitting enough your policy to be executed for every single component, even if the license of a component does not require the obligation expressly.

9 generic obligations in the core

Name	Category	Lead	Nb of licenses	Passivity	Actions
License agreement disclaiming responsibility of other contributors	License agreement	Legal	7	Active	
Preserve IP mentions in Source code	Mentions	DevQA	212	Active	
License and copyright notices in documentation	Mentions	DevQA	174	Active	
Display copyright and licence in Program	Mentions	DevQA	41	Active	
No use of names for endorsement	Communication constraints	Communication	87	Passive	
Patent Peace	IP management	Legal	44	Passive	
Marking Modifications	Mentions	DevQA	100	Active	
Libraries must stay libraries	Technical constraints	DevQA	4	Active	
Respect trademarks	Communication constraints	Communication	65	Passive	

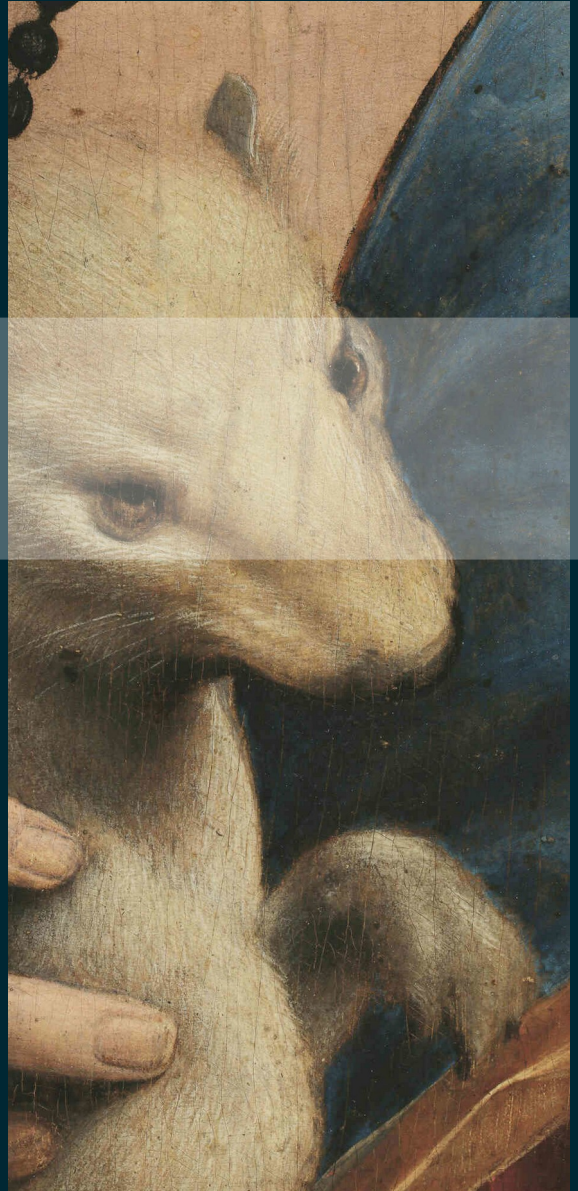
19 generic obligations out of the core

Name	Category	Lead	Nb of licenses	Passivity	Actions
BadgeWare	Mentions	DevQA	6	Passive	
License agreement does not attempt to limit rights given by upstream	License agreement	Legal	26	Passive	
Don't sell the software in itself	License agreement	Legal	5	Passive	
Strong Copyleft	IP management	Legal	19	Active	
Inability to Comply Due to Statute or Regulation	IP management	Legal	20	Active	
Weak Copyleft	IP management	Legal	58	Active	
Providing Modifications to original author	Providing source code	DevQA	7	Active	
SaaS : mentions	Mentions	DevQA	2	Active	

We validate SBOMS

- Validation in 5 steps:
  1) Presence of **valid SPDX** licence expression;
  2) **“AND”s** are actual “AND”s and not “OR”s;
  3) **Type of exploitation** has been decided for every dependency;
  4) **Choices** (e.g. “MIT OR GPL-2.0-only”) have been decided;
  5) All licences have been **reviewed** by the legal department.
- We handle generalisation of decisions.

Brainstorming



Thanks !

https://hermine-foss.org/

- See the project website here: https://hermine-foss.org
- The code is available under the AGPL-3.0-only at: https://gitlab.com/hermine-project/hermine
  - A first small set of analyzed licences/generic obligations is available in the repo
- The documentation is available under the CC-BY-4.0 license at: https://docs.hermine-foss.org