

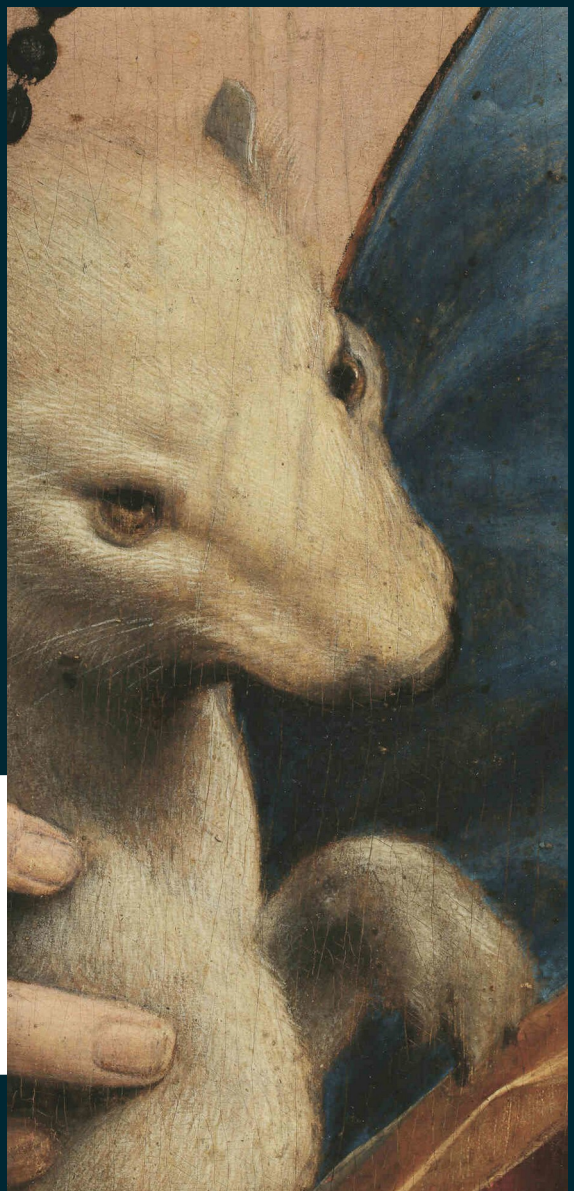
The Hermine Project

Automate legal compliance with Hermine

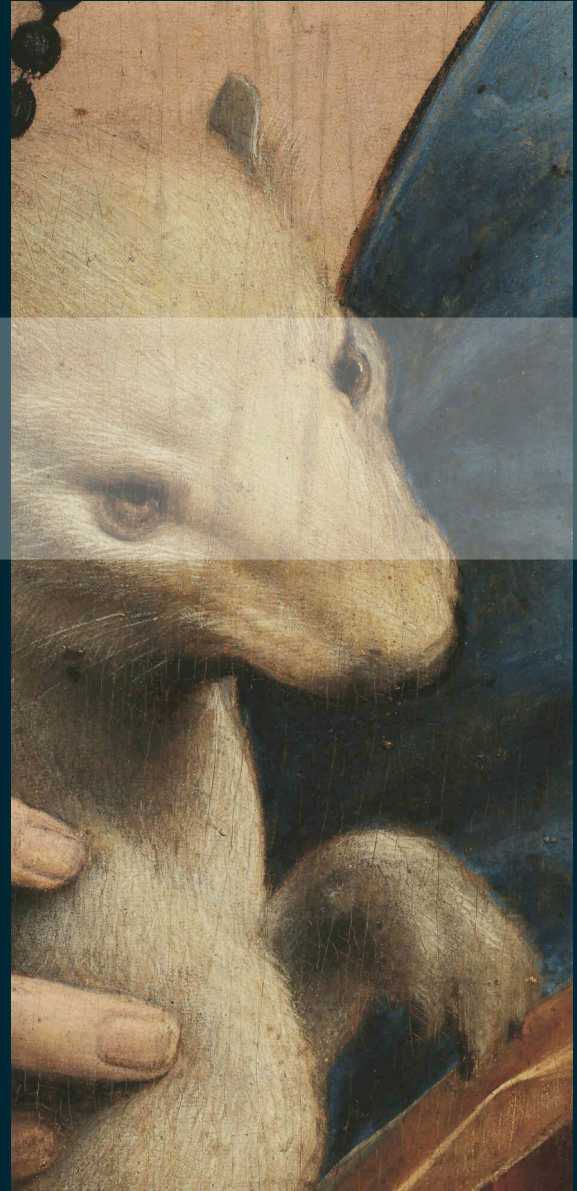


June 15th, 2023

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

<https://hermine-foss.org/>

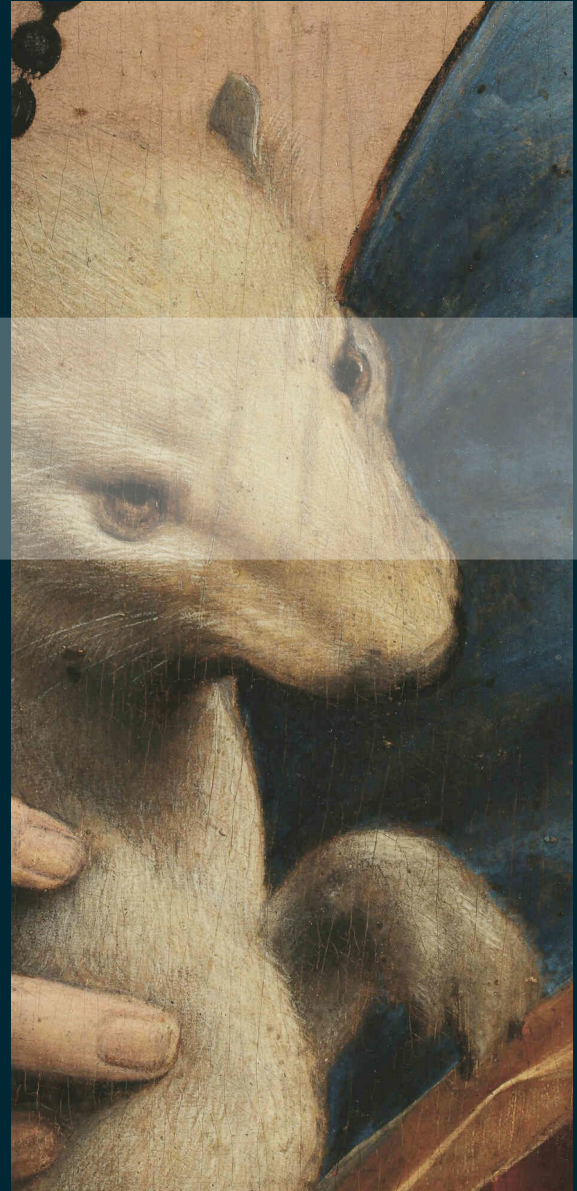


The general spirit towards compliance

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

The image displays two screenshots of the Hermine application interface. The left screenshot shows the 'Edit' page for the 'LGPL-2.0-or-later' license, with a sidebar menu on the left containing options like Dashboard, Your products, Components, Licenses, Generic obligations, Authorized contexts, Derogations, License choices, API, Django Admin, and About. The right screenshot shows the 'Edit' page for the 'BSD-3-Clause' license, displaying a table of main characteristics and a list of obligations attached to the license.

HERMINE

GENERAL

Dashboard

DEVELOPMENT

Your products

Components

LEGAL

Licenses

Generic obligations

Authorized contexts

Derogations

License choices

TOOLS

API

Django Admin

About

Hermine / Licenses / BSD-3-Clause

Edit this license Actions

BSD 3-Clause "New" or "Revised" License

LICENSE

Main characteristics of this license

SPDX identifier: BSD-3-Clause (Other URL)	Copyright: Patent-free	Choice of law: None
Review status: To check	Actually FOSS: FOSS - default	Choice of venue: None
FOSS policy status: Always allowed	Patent Grant: No	Disclaimer of Warranty: Unknown
Explanation of FOSS policy: <i>No explanation has been given for this OSS policy - Edit</i>	Ethical clause: No	Limitation of Liability: Unknown
	Restricted to non-commercial use: No	Comment: <i>no comment</i>
		✓ This license is covered by the obligations in the core

Obligations attached to this license

Attach new obligation

Obligations related to Mentions

Licence dans la documentation (Active) Edit obligation Delete obligation

Related to generic obligation: [\[Core\]License and copyright notices in documentation](#)

Applies:

- Whether the component is modified or not
- If the component is distributed as binary

• Corresponding text in the license:

Conservation des mentions de PI dans source (Active) Edit obligation Delete obligation

Related to generic obligation: [\[Core\]Preserve IP mentions in Source code](#)

Applies:

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.

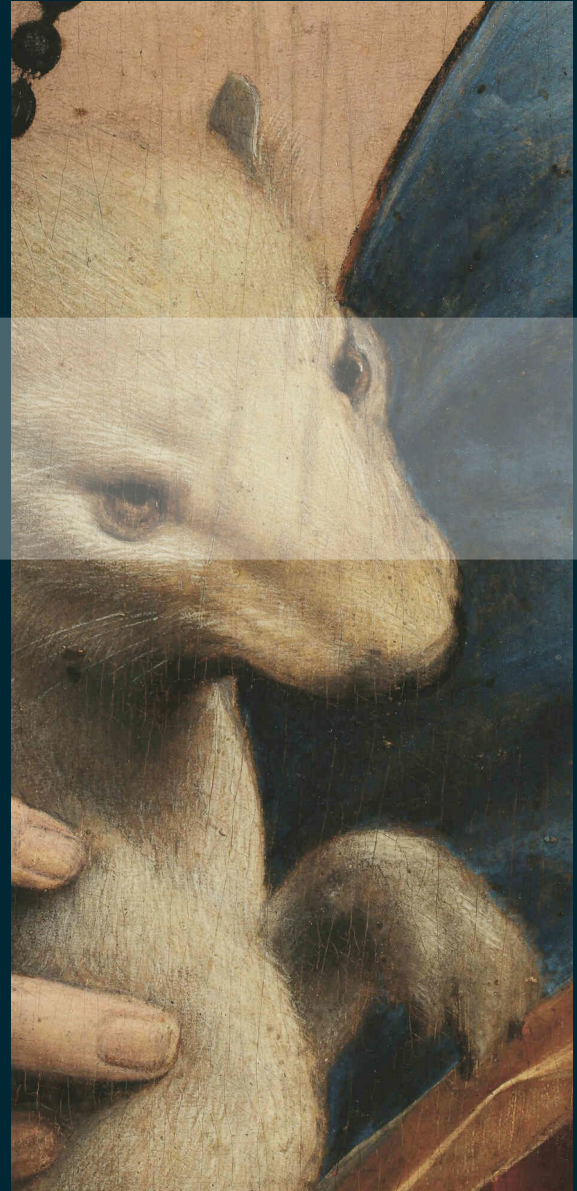
🔗 9 generic obligations in the core					
Name	Category	Lead	Nb of licenses	Passivity	Actions
License agreement disclaiming responsibility of other contributors	License agreement	Legal	7	Active	🔍 🗑️
Preserve IP mentions in Source code	Mentions	Dev-QA	212	Active	🔍 🗑️
License and copyright notices in documentation	Mentions	Dev-QA	174	Active	🔍 🗑️
Display copyright and licence in Program	Mentions	Dev-QA	41	Active	🔍 🗑️
No use of names for endorsement	Communication constraints	Communication	87	Passive	🔍 🗑️
Patent Peace	IP management	Legal	44	Passive	🔍 🗑️
Marking Modifications	Mentions	Dev-QA	100	Active	🔍 🗑️
Libraries must stay libraries	Technical constraints	Dev-QA	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	Dev-QA	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	Dev-QA	7	Active	🔍 🗑️
SaaS - mentions	Mentions	Dev-QA	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>