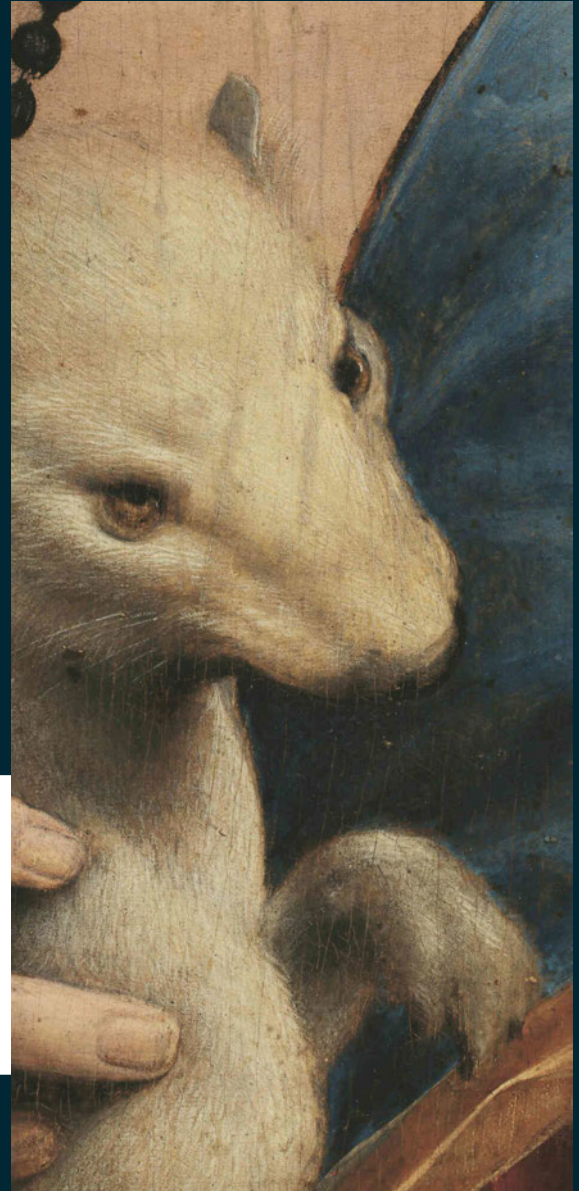


The Hermine Project

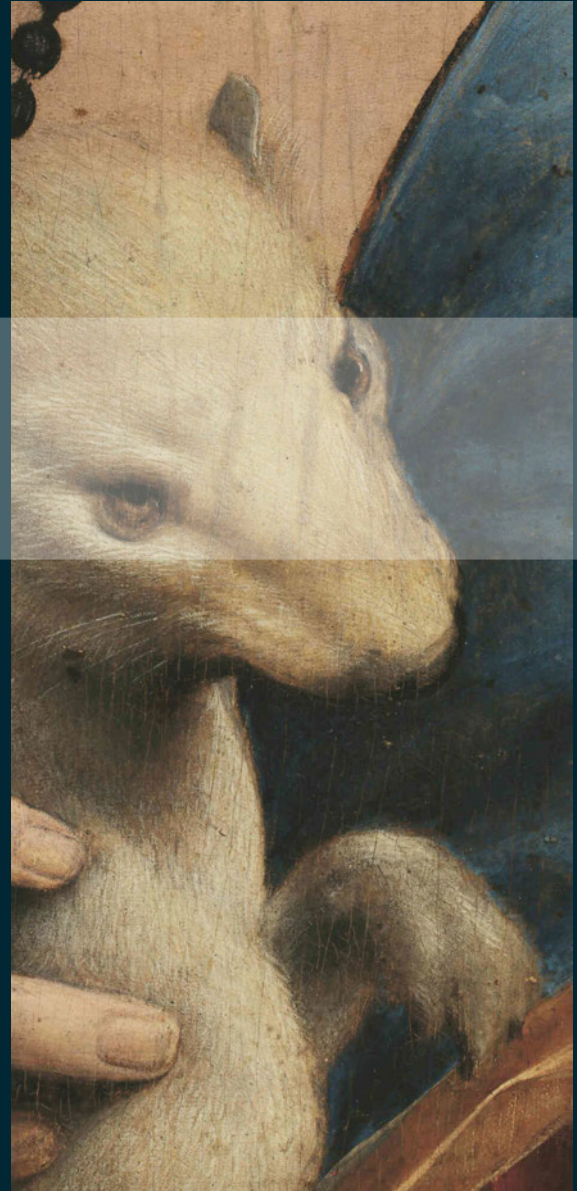
*Automating open
source compliance*

CW2
con'23

June 15th, 2023



Why Hermine ?



Context

FOSS is everywhere

... and a **concern for any IP lawyer**, not only
FOSS lawyers

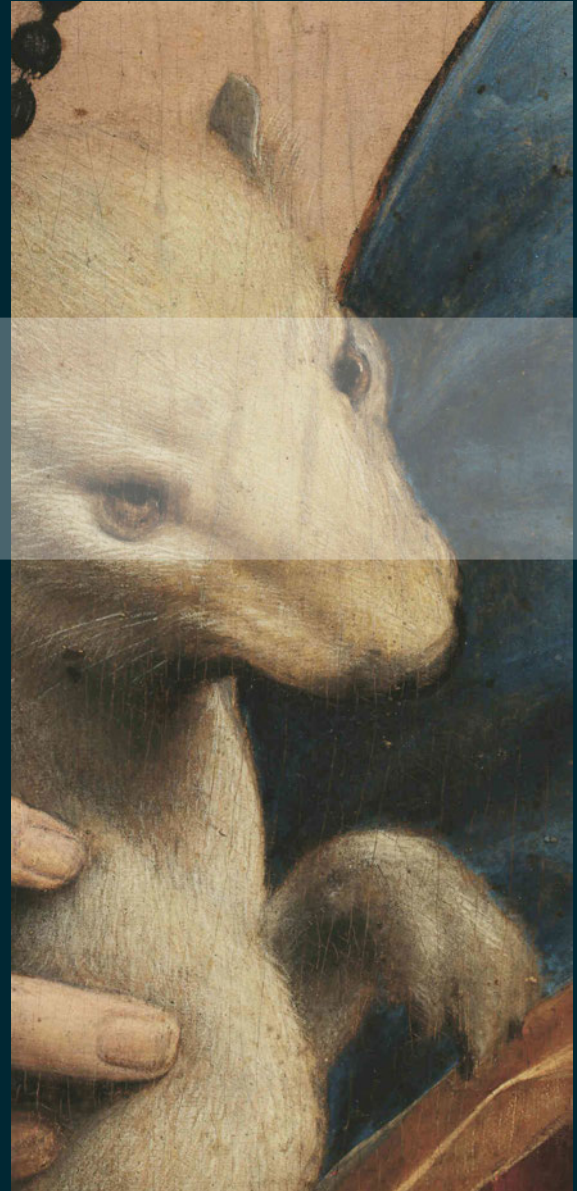
Many **needs are common** across organisations

Context

In the open source ecosystem:

- many tools to produce SBoMs
- that can sometimes apply predefined rules
- but no project could really embrace the complexity of a complete FOSS Compliance Policy

Objectives



Goal

Ease application of FOSS compliance policies

- For any organisation: foundations, companies, ...
- Unique solution for all: lawyers, compliance officers, ...
- Interface with existing Open Source tools

Goal

Hermine answers 2 main questions:

- 1) Can I use that component in this product ?
- 2) What obligations must I fulfill to distribute that component ?

The spirit

Efficient and pragmatic

+

Limit legal uncertainty

→ Each organisation decides on the **level of risk** it considers acceptable.

Licence analysis database

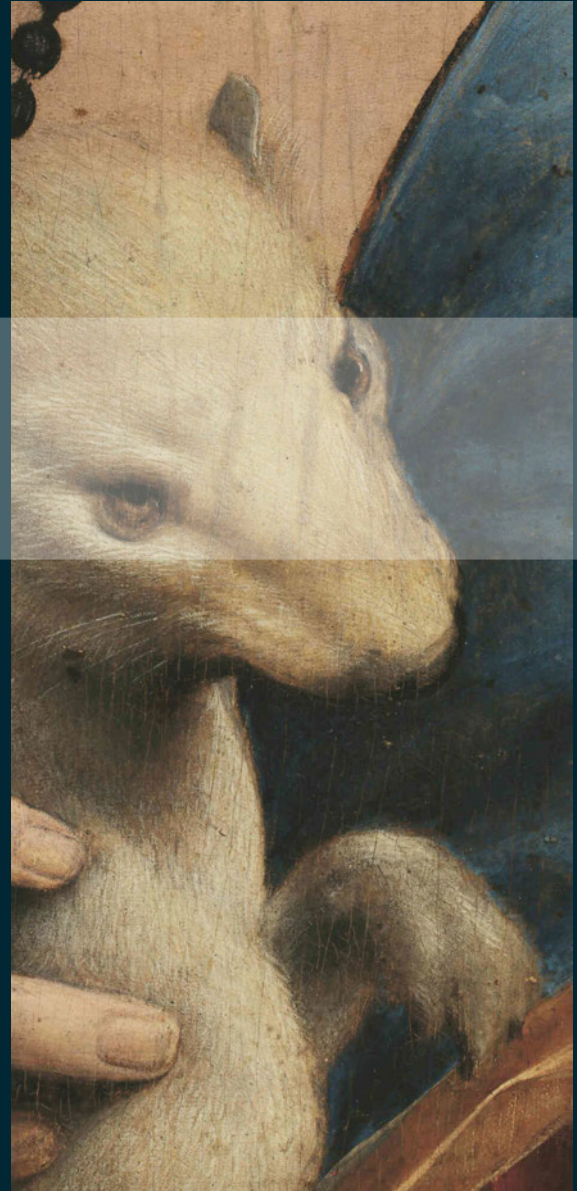
Provide a framework to **work on** and **share** legal licence analysis.

Still, users have **complete privacy** over:

→ their own interpretation of the licences

→ their own open source policies

How ?



The big picture

INPUT

Organisation
level

FOSS Compliance Policy

Project
level

List of dependencies (SBoM)

Business Context

Dependency
level

How it is distributed

If it was modified

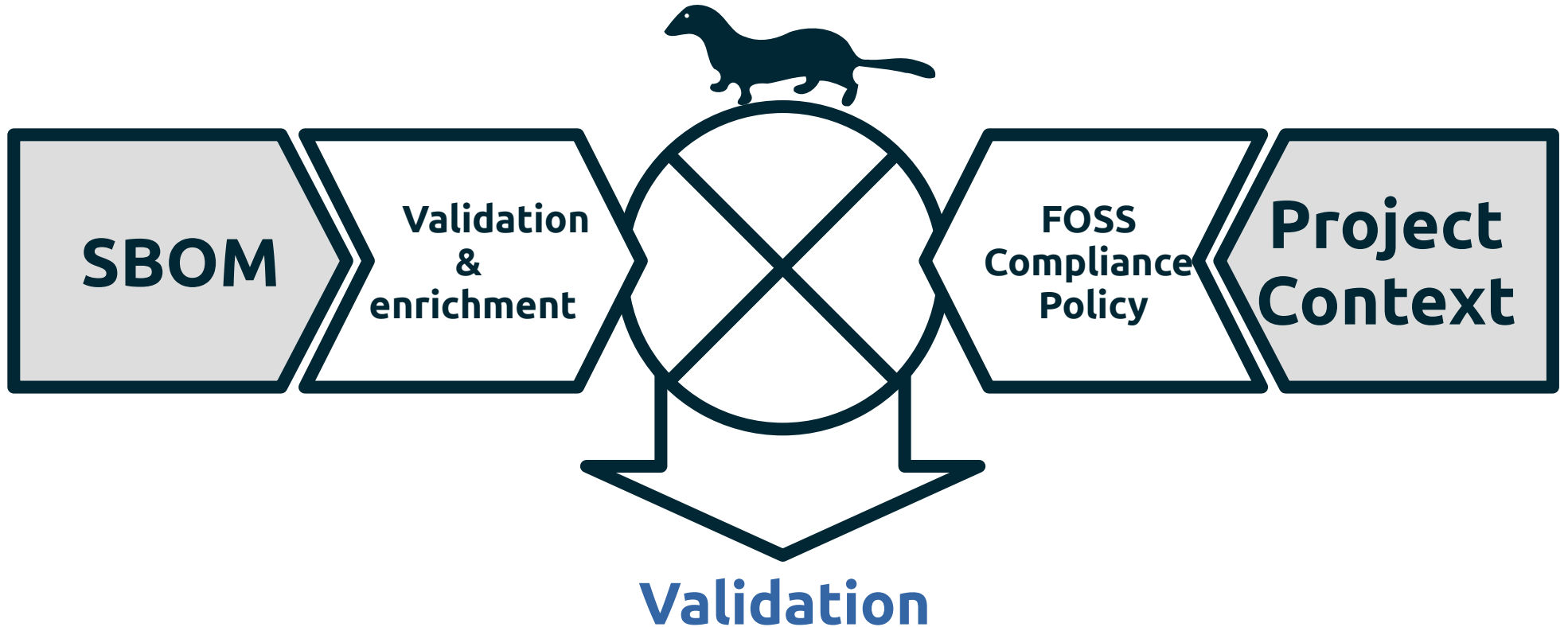
How it is linked to the main program

The big picture

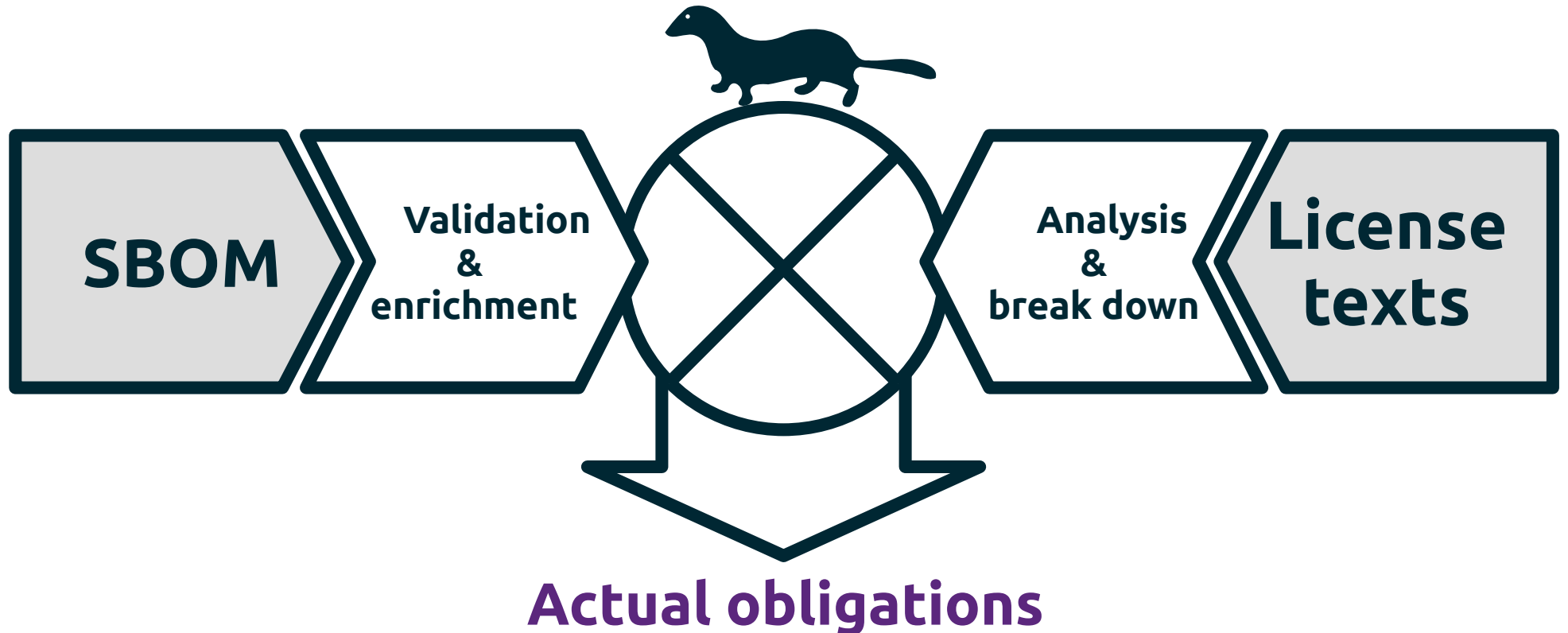
OUTPUT

- 1) Dependencies licences validation with respect to context
- 2) List of resulting obligations

The big picture



The big picture



Project Organisation

- Started by six, end-user, partner companies in a semi-formal context.
- 3 committees (legal, technical, steering)
- Code under AGPL-3.0-only, Data under OdbL-1.0



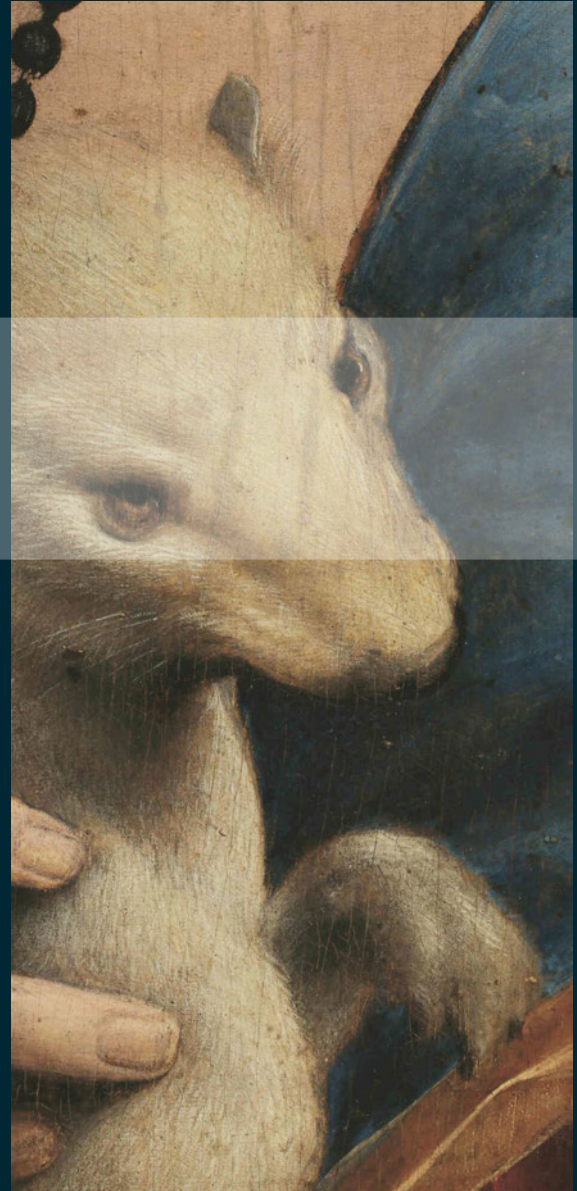
Technical implementation

- Python / Django framework
- REST API (DRF)
- BDD agnostic but PostgreSQL preferred

Code: <https://gitlab.com/hermine-project/hermine>

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

Where we are
+
Roadmap



Already here

Main features:

- Licence analysis for contextual validation
- ORT/SPDX import
- Role management
- 5 step validation with choices storage (curations, etc.)
- Resulting obligations
- Component / products catalog

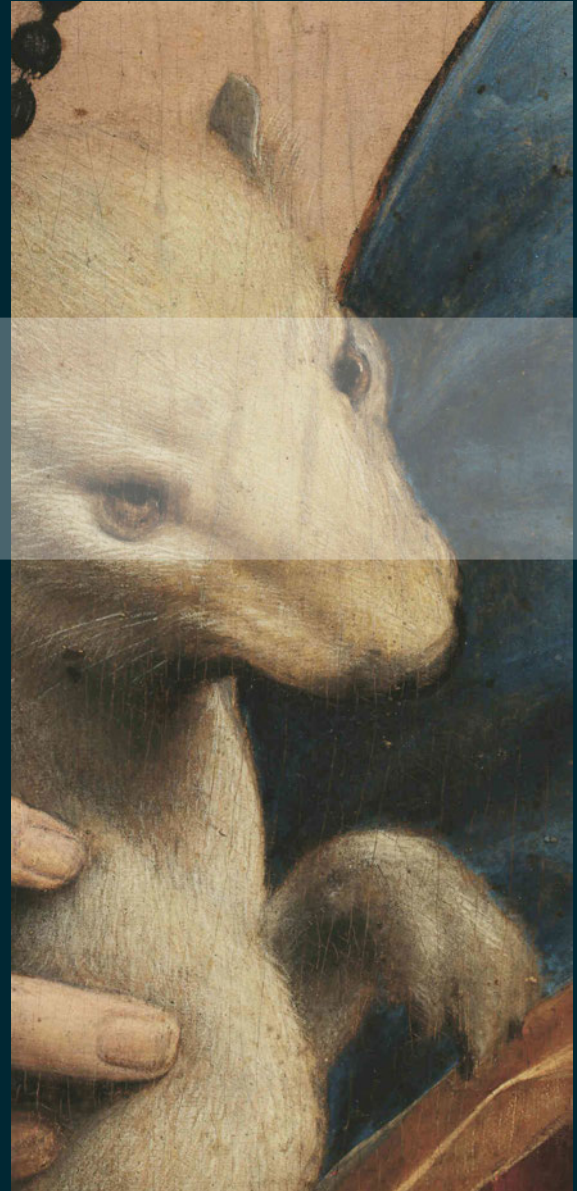
Being implemented for next step (1.0)


- Data sharing (licences interpretation)
- Deployment automation
- Better UX/UI
- Better documentation
- Global Hardening / testing

Next ?

- Interested ? Come join us !
- Curious ? Come chat with us
- Join us at the **breakout session this afternoon**

Annex: Screenshots



 459 Licenses

SPDX ID	License name	Policy status	# of obligations
CDLA-Sharing-1.0	Community Data License Agreement Sharing 1.0	Not reviewed yet	
CECILL-1.0	CeCILL Free Software License Agreement v1.0	Never allowed	7 obligations
CECILL-1.1	CeCILL Free Software License Agreement v1.1	Never allowed	7 obligations
CECILL-2.0	CeCILL Free Software License Agreement v2.0	Never allowed	7 obligations
CECILL-2.1	CeCILL Free Software License Agreement v2.1	Never allowed	7 obligations
CECILL-B	CeCILL-B Free Software License Agreement	Always allowed	8 obligations
CECILL-C	CeCILL-C Free Software License Agreement	Allowed depending on context	8 obligations
CERN-OHL-1.1	CERN Open Hardware Licence v1.1	Not reviewed yet	
CERN-OHL-1.2	CERN Open Hardware Licence v1.2	Not reviewed yet	
CERN-OHL-P-2.0	CERN Open Hardware Licence Version 2 - Permissive	Not reviewed yet	
CERN-OHL-S-2.0	CERN Open Hardware Licence Version 2 - Strongly Reciprocal	Not reviewed yet	
CERN-OHL-W-2.0	CERN Open Hardware Licence Version 2 - Weakly Reciprocal	Not reviewed yet	
CLArtistic	Clarified Artistic License	Allowed depending on context	5 obligations
CNRI-Jython	CNRI Jython License	Always allowed	5 obligations
CNRI-Python	CNRI Python License	Always allowed	3 obligations

Mozilla Public License 1.0

 LICENSE

Main characteristics of this license

SPXD identifier: [MPL-1.0](#) 

Review status: Checked

FOSS policy status:
Allowed depending on context

Copyleft: Weak copyleft

Actually FOSS: FOSS - deduced

Patent Grant: Yes

Ethical clause: No

Restricted to non-commercial use: No

Choice of law: **California law**

Choice of venue: **Federal Courts of the Northern District of California, with venue lying in Santa Clara County**

Disclaimer of Warranty: **Full clause**


Limitation of Liability: **Full clause**

Licenses involved in this release

Apache-2.0 BSD-3-Clause LGPL-2.1-or-later MIT MPL-2.0

List of generic obligations to follow

In core?	Generic name	Lead	Metacategory	Passivity	Components
Not in core	License agreement does not attempt to limit rights given by upstream	Legal	LicenseAgreement	Passive	Concerned components
Not in core	Inability to Comply Due to Statute or Regulation	Legal	IPManagement	Active	Concerned components
Not in core	Weak Copyleft	Legal	IPManagement	Active	Concerned components
Not in core	Providing CSC to end user	DevQA	ProvidingSourceCode	Active	Concerned components
Not in core	Indemnification of contributors	Legal	LicenseAgreement	Active	Concerned components
Not in core	License Agreement must exclude other contributors for additionnal terms	Legal	LicenseAgreement	Active	Concerned components
In core	Preserve IP mentions in Source code	DevQA	Mentions	Active	Concerned components
In core	License and copyright notices in documentation	DevQA	Mentions	Active	Concerned components
In core	Display copyright and licence in Program	DevQA	Mentions	Active	Concerned components
In core	No use of names for endorsement	Communication	Communication	Passive	Concerned components
In core	Patent Peace	Legal	IPManagement	Passive	Concerned components
In core	Libraries must stay libraries	DevQA	TechnicalConstraints	Active	Concerned components
In core	Respect trademarks	Communication	Communication	Passive	Concerned components

 Top 50 Most used components

Type	Name	Number of usages	Description	Funding opportunity
npm	debug	6	small debugging utility	
npm	ms	6	Tiny milisecond conversion utility	
npm	supports-color	4	Detect whether a terminal supports color	
maven	org.javassist/javassist	3	Javassist (JAVA programming ASSISTant) ma...	
npm	p-limit	3	Run multiple promise-returning & async fu...	
maven	jfree/jcommon	3	JCommon is a free general purpose Java cl...	
npm	escape-string-regexp	3	Escape RegExp special characters	
npm	p-locate	3	Get the first fulfilled promise that sati...	
npm	find-up	3	Find a file by walking up parent director...	
npm	minimatch	3	a glob matcher in javascript	
npm	semver	3	The semantic version parser used by npm.	