



LLW  
2024

## Hermine:

Open Source compliance  
with an automated,  
community-driven tool

# Vision & history

A community-driven approach for (mostly FOSS) licences understanding

- Building a **common way of complying with Open Source Licences**. We want every (non FOSS Expert) lawyer to benefit from open source best practices/knowledge and adapt these practices to their specific needs.
- **Our challenge** : to design a digital common (both a software, a database and a community of practice) that allows any lawyer to comply with any Open Source Obligation.
- in line with the dynamics of OS licences from the beginning (general licences, reuse of clauses, use of exceptions, etc.).



# Vision & history

Our methodology:

## 1) Building a **consensus** :

- which would bring a community-driven shared understanding of licences WHILE still allowing flexibility for private reinterpretation within each organisation
- Concretely, we worked on the methodology of analysis (defining a common "canvas") and the result of the application of this methodology by a community of (non FOSS experts) lawyers (the reference consensus).

## 2) with a **automated application** in mind:

- at the level of licence analysis and at at the level of application,
- Applying the FOSS policies (integrating compliance in CI/CD processes).



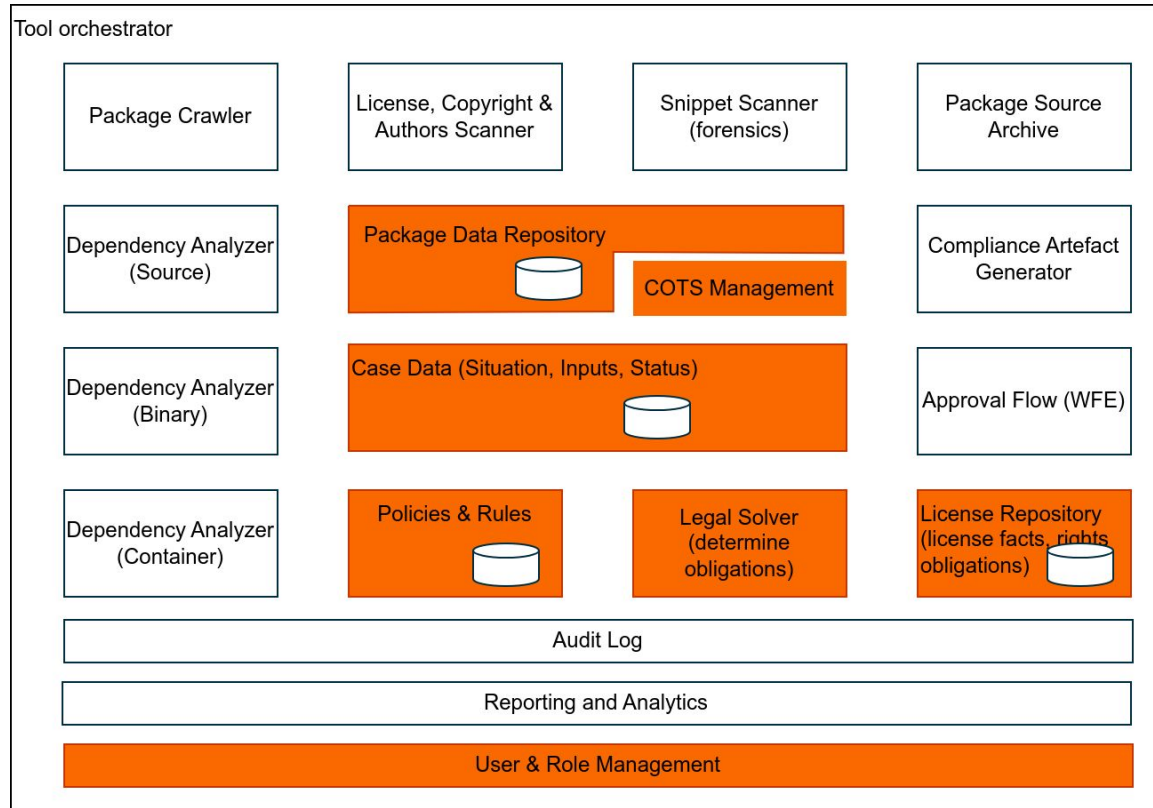
# Vision & history

## Our mindset:

- FOSS and Open Data
- End-user-driven project (Lectra, Orange, OVH Cloud, Enedis, RTE, inno<sup>3</sup>)
- Don't reinvent the wheel / on the shoulders of giants
- A scope as small as possible / as large as necessary



# Where we are on the map



# Standards we rely on

- For licence IDs: SPDX + NexB's/DejaCode LicenseRef-s
- SBOMs: ORT's evaluated model (scopes !)+ SPDX (+ CyclonDX ASAWHT)
- For Components IDs: PURL
- For curations: ORT's format (still WIP)
- Licence analysis data: Goal is to converge AMAP with OSADL (not that simple) (and others FOSSlight, etc.)



# Licence analysis

- Main characteristics :
  - Copyleft, Patent grant, Choice of law
  - Foss policy status
- Obligations
  - Passive / Active
  - Trigger :
    - Modification status
    - Exploitation (distribution source / non-source)
  - **Related Generic obligation**



## Main characteristics of this license

SPDX identifier: [AGPL-3.0-only](#) [\(Other URL\)](#) Copyleft

Review status: To check Actually

FOSS policy status: Never allowed Patent

Explanation of FOSS policy: Ethical

*No explanation has been given for this OSS policy - [Edit](#)* Restrict

## Obligations attached to this license

### Obligations related to Technical constraints

Non tovoization (Active)

Related to generic obligation: [Non Tivoization](#)

Applies:

# Licence analysis : policy status

- Always/ Never / Depends on the context :
- « Authorized contexts » :
  - Technical criteria: exploitation, modification, linking type
  - « Business » criteria : the category of your product

## Authorized contexts:

There is 2 generic contexts authorized for this license (listed below) and 0 product-specific derogations.

Linking	Modification	Exploitation	Product category	Scope	Justification
Any	Any	Any	R&D	Any	R & D products can have code published ur
Any	Any	Any	Linux embarqué	kernel space	Embedded Linux makes GPLv2 mandatory

+ Add an authorized context



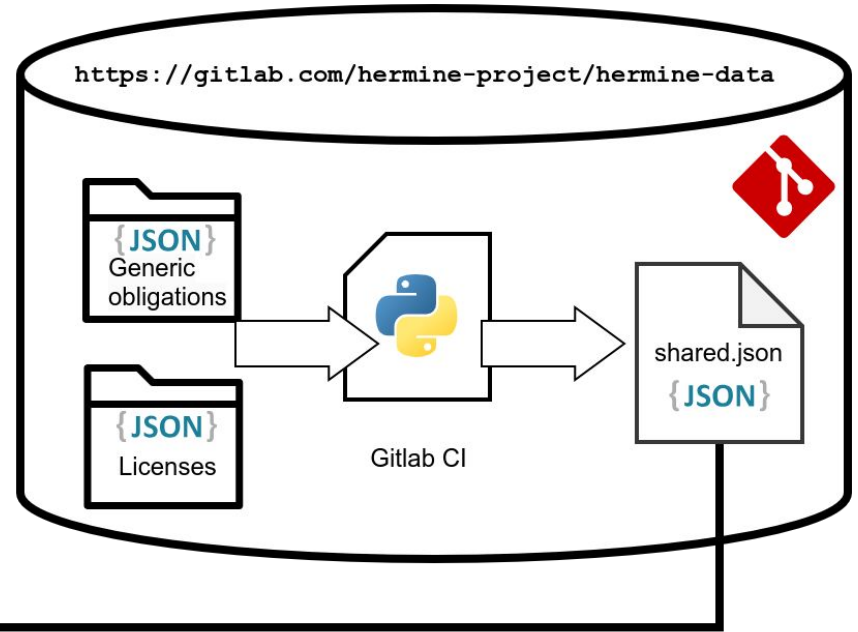
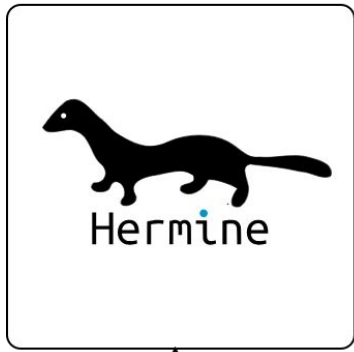


# Generic obligations

- Grouping obligations from licences considered functionnally equivalent and that could be handled by the same process.
  - « The name of the Copyright Holder may not be used to endorse or promote products derived from this software without specific prior written permission. » (Artistic-1.0)
  - « Neither the name of the copyright holder nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. » (BSD-3-Clause)



# Using reference data



# Using reference data

## Shared reference data

### Licenses

Total	462
Different from shared data	219
Absent from shared data	4

7 licenses present in the shared database are missing from local data

Sync 7 licenses

This will also copy any linked obligation or generic obligation.

### Generic obligations

Total	29
Different from shared data	5
Absent from shared data	0

2 generics present in the shared database are missing from local data

Sync 2 generics

Apache-1.1	Apache License 1.1	Always allowed	5 obligations	To check	Local only
Apache-2.0	Apache License 2.0	Always allowed	7 obligations	To check	See differences
APAFML	Adobe Postscript AFM License	Always allowed	0 obligations	To check	Local only
APL-1.0	Ada 1.0				

Apache License 2.0

### License analysis

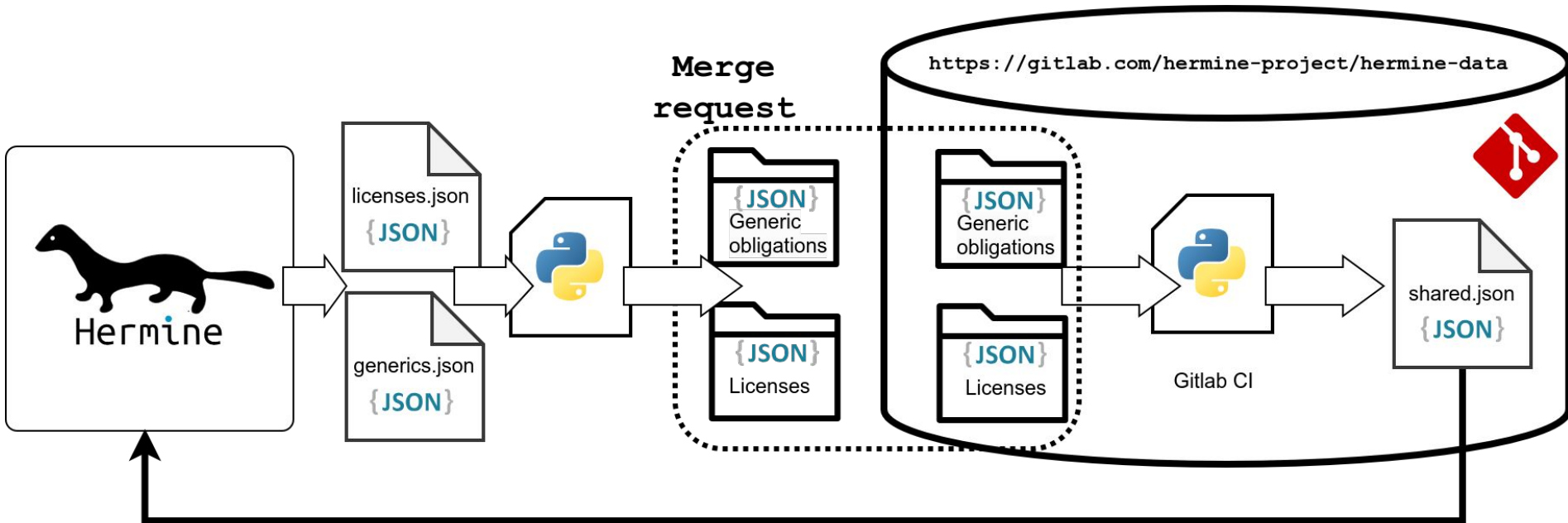
Field	Reference	Local value	Actions
Patent grant	True	False	Update local field

### Obligations

Name	Field	Reference	Local value	Actions
License and notices in Source code	Generic	Preserve IP mentions in Source code	Preserve legal mentions in source code	Update local field
Patent peace			Only in local database	



# Contributing to reference data (WIP)



# Thanks !

## Questions ?

Front page photo Statyn "Poseidon med brunnskar" på Götaplatsen i Göteborg. Utförd av Carl Milles.

(c) <https://commons.wikimedia.org/wiki/User:Historiker> under CC-BY-SA-3.0



# Ingesting, validating data

- Importing raw SBOMS
- Adding information
- Validating data (curations / choices)

