Bildlizenz: imaginima/E+ via Getty Images

# SBOM Management at Mercedes-Benz

Dr. Christian Wege, Dr. David Schumm of Mercedes-Benz Group AG

Bitkom Forum Open Source 2023
Erfurt, 27.09.2023

Mercedes-Benz

# Agenda

With the **FOSS Disclosure Portal** we aim at a more efficient, digital, and transparent software supply chain regarding open source

## Mission

**Free & Open Source Software (FOSS)** brings innovation, efficiency and speed, but we need to make sure to play it save

## FOSS Disclosure Portal

**Software Bill of Materials (SBOM)** provided by suppliers to our central inventory enables **checking** license conformance easier & faster

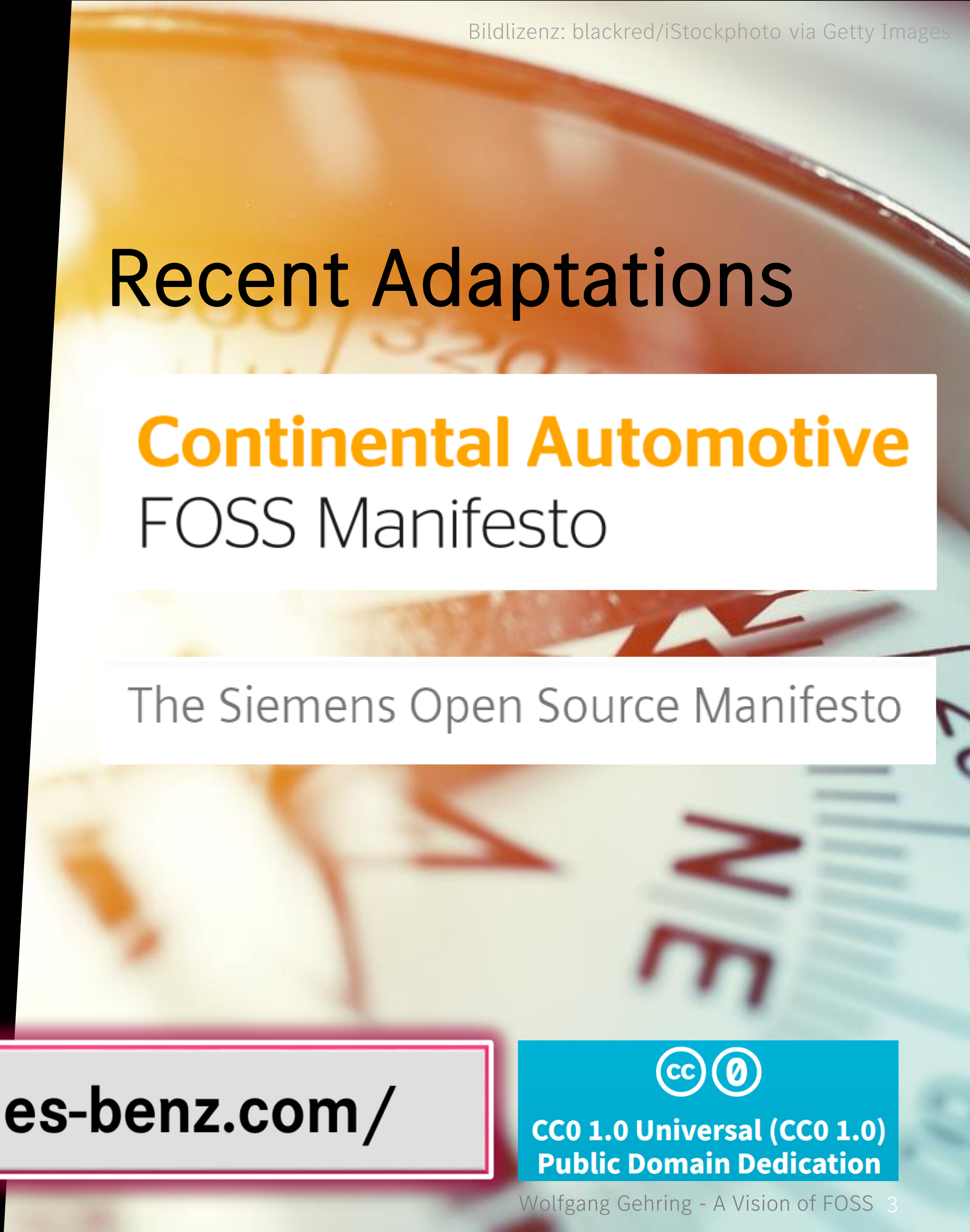
## SBOM Management at Scale

**FOSS SBOM consumption** will intensify the collaboration with software suppliers and poses both opportunities and challenges

# Mercedes-Benz FOSS Manifesto

- Set of guidelines which proclaim the importance of FOSS for a modern tech organization
- Consists of three parts: Preamble, Company Principles, Employee Principles
- Goal: Facilitate the cultural change in Mercedes-Benz IT & our subsidiaries towards Inner Source and Open Source
- Sends our engineers on their FOSS Mission

→ **https://opensource.mercedes-benz.com/**



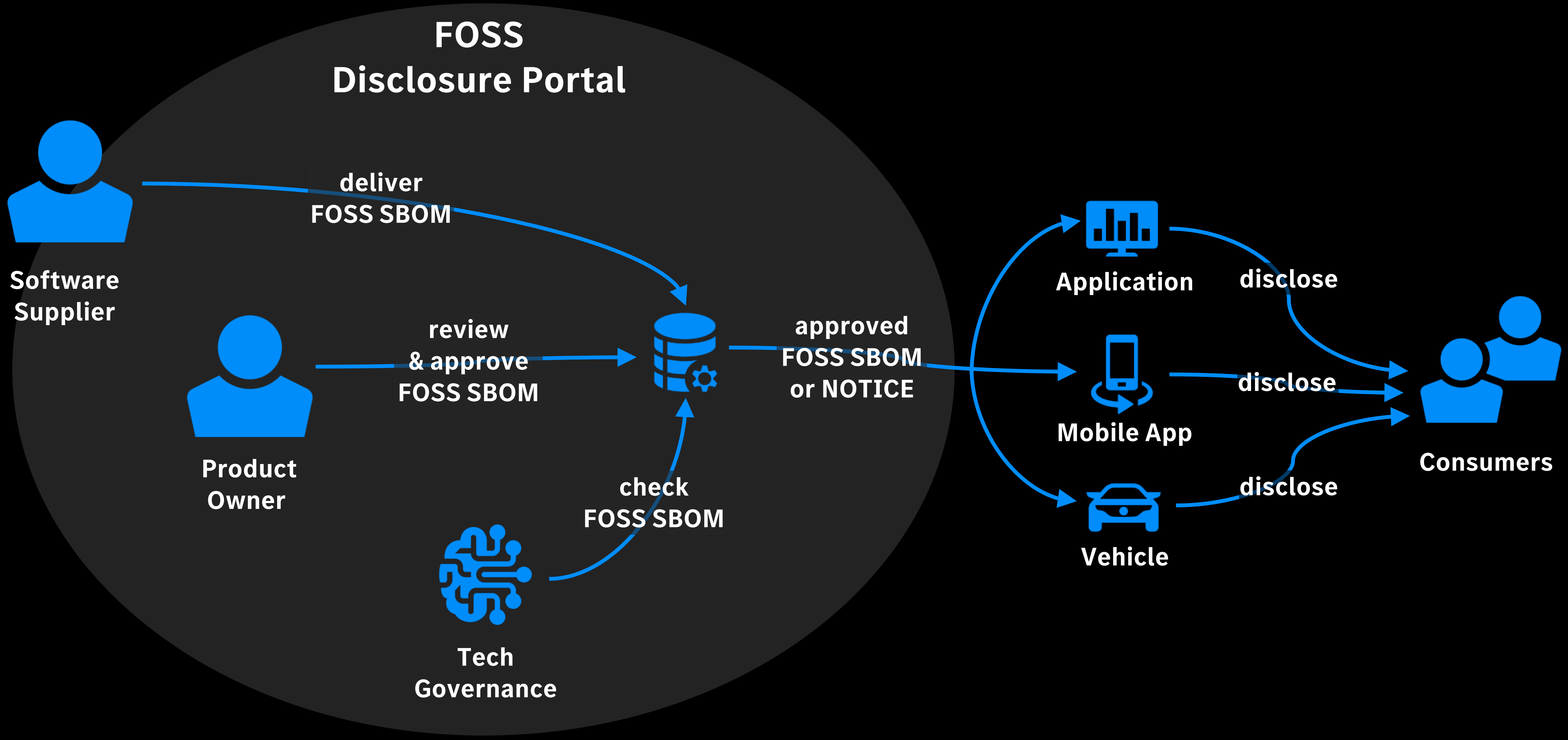
Bildlizenz: blackred/iStockphoto via Getty Images

## Recent Adaptations

**Continental Automotive**
FOSS Manifesto

The Siemens Open Source Manifesto

# FOSS SBOM in the Software Supply Chain



# Open Source Options

Use one of these ...

OSS Review Toolkit

FOSSLIGHT

Hermine

dependency track

SW360

... or build your own

Bildlizenz: Christian Horz/iStockphoto via Getty Images

# FOSS Disclosure Portal

## OUR VISION: WHAT IS IT?

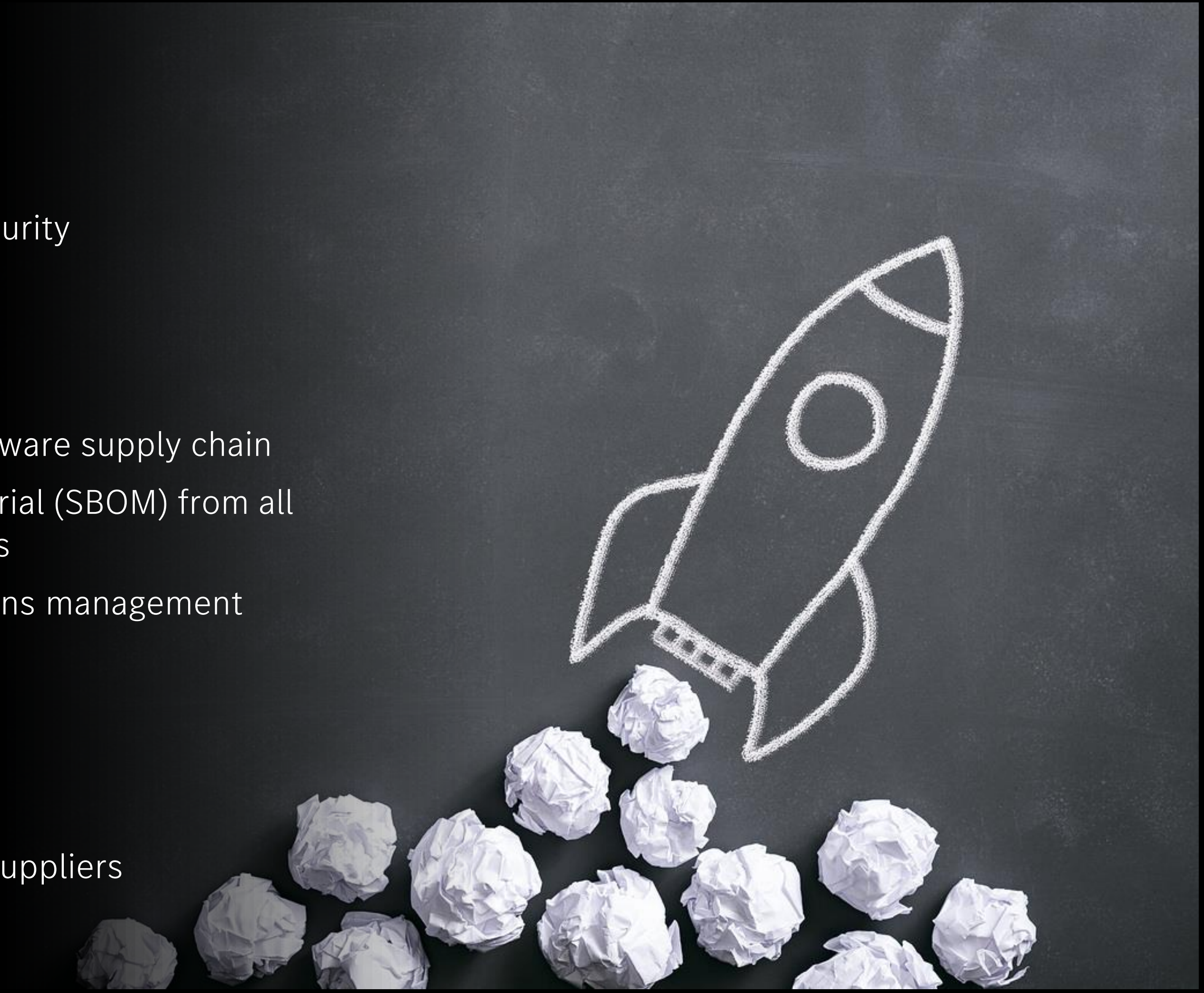
- A more efficient, transparent and digital software supply chain
- Digitized and automated FOSS Disclosure Process
- Increased transparency leads to better license compliance and security

## OUR MISSION: HOW DO WE ACHIEVE IT?

- With the FOSS Disclosure Portal we automate the open source software supply chain
- Create a central worldwide inventory of FOSS Software Bill of Material (SBOM) from all Mercedes-Benz companies with legal information for license checks
- Provide automation for guided conformance checking and obligations management

## OUR PURPOSE: WHY DO WE STRIVE FOR IT?

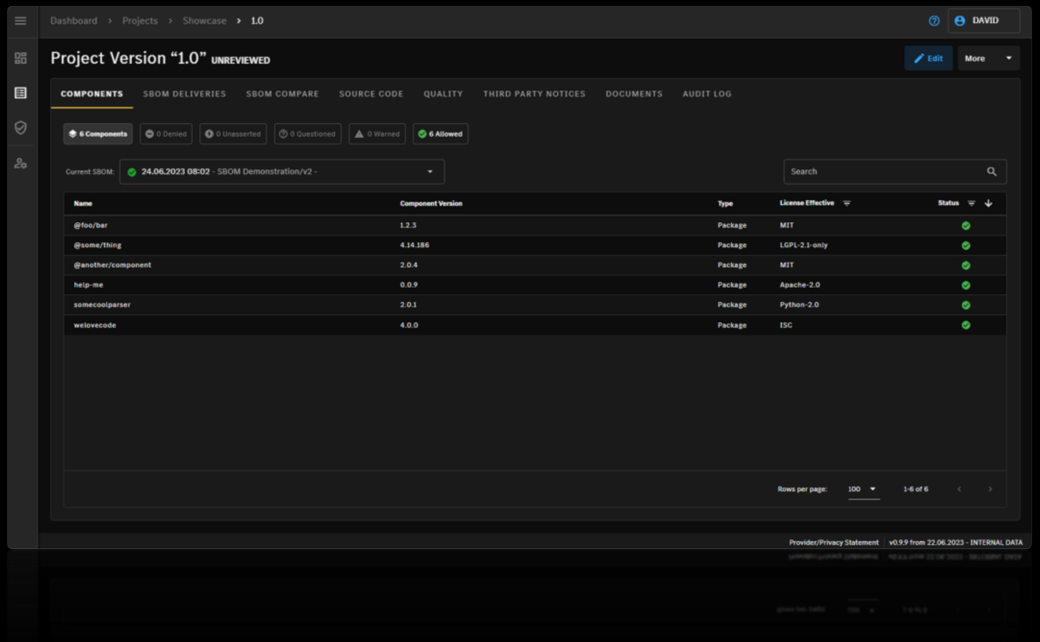
- Be compliant, secure, and developer-friendly
- Make life easier for developers, application owners, and software suppliers
- Follow the company's software compliance guidelines



Bildlizenz: ThomasVogel/iStockphoto via Getty Images

# Benefits for Product Owners

ISO Format for
SBOM Exchange



Project Version “1.0” UNREVIEWED

Current SBOM: 24.06.2023 08:02 - SBOM Demonstration/v2 -

| Name | Component Version | Type | License Effective | Status |
|---|---|---|---|---|
| @foo/bar | 1.2.3 | Package | MIT | ✓ |
| @some/thing | 4.14.186 | Package | LGPL-2.1-only | ✓ |
| @another/component | 2.0.4 | Package | MIT | ✓ |
| help-me | 0.0.9 | Package | Apache-2.0 | ✓ |
| somecoolparser | 2.0.1 | Package | Python-2.0 | ✓ |
| welovecode | 4.0.0 | Package | ISC | ✓ |

Rows per page: 100 1-6 of 6

v0.9.9 from 22.06.2023 - INTERNAL DATA

UI/UX Design
for Ease of Use

REST API & CLI for
CI/CD Integration

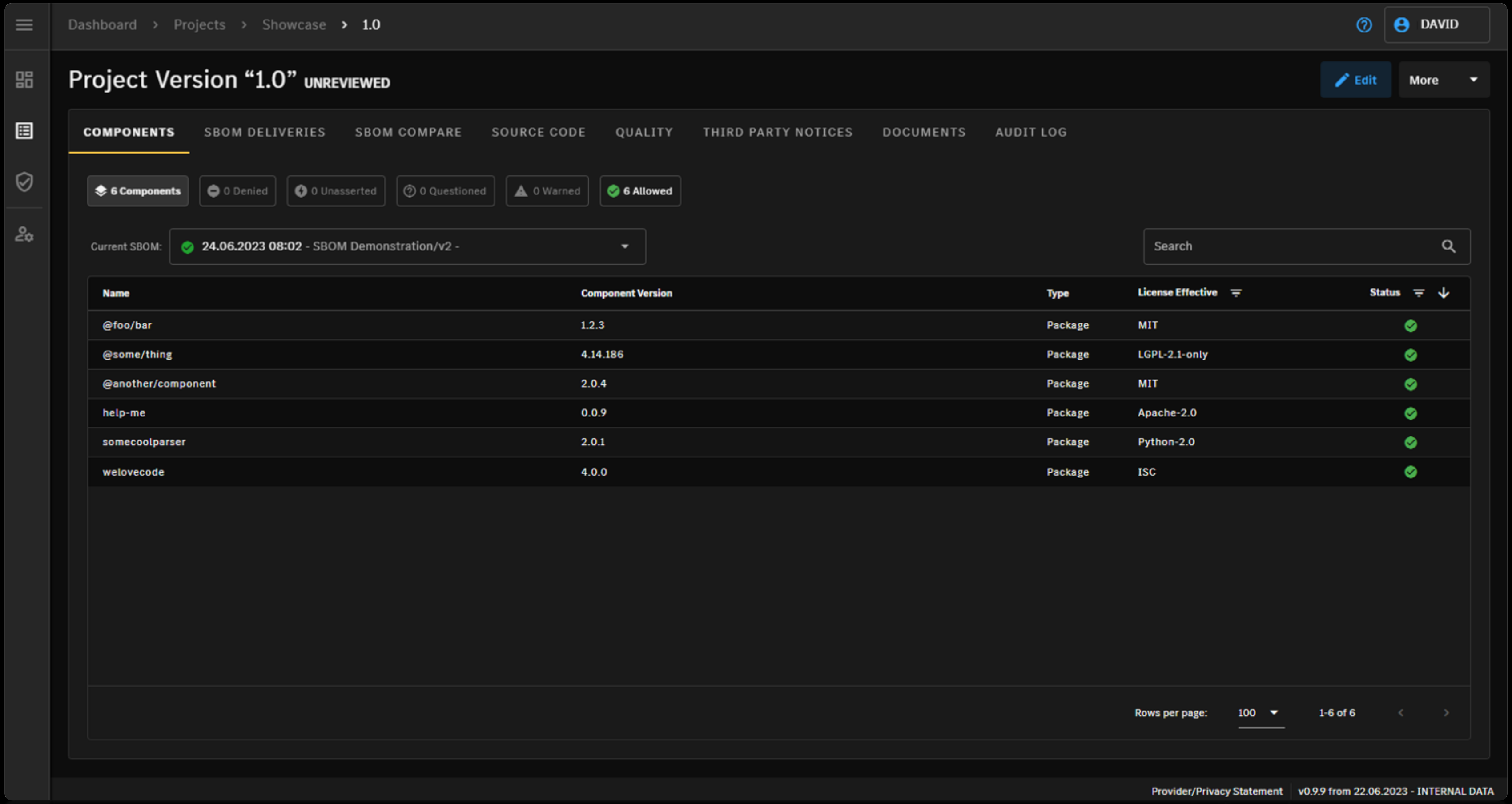
Notice Generation
for Disclosure

License Database
for Legal Guidance

Policy Rules for
Compliance

Quality Checks for
Obligations Management

# Demo



Project Version “1.0” UNREVIEWED

Current SBOM: ✓ 24.06.2023 08:02 - SBOM Demonstration/v2 -

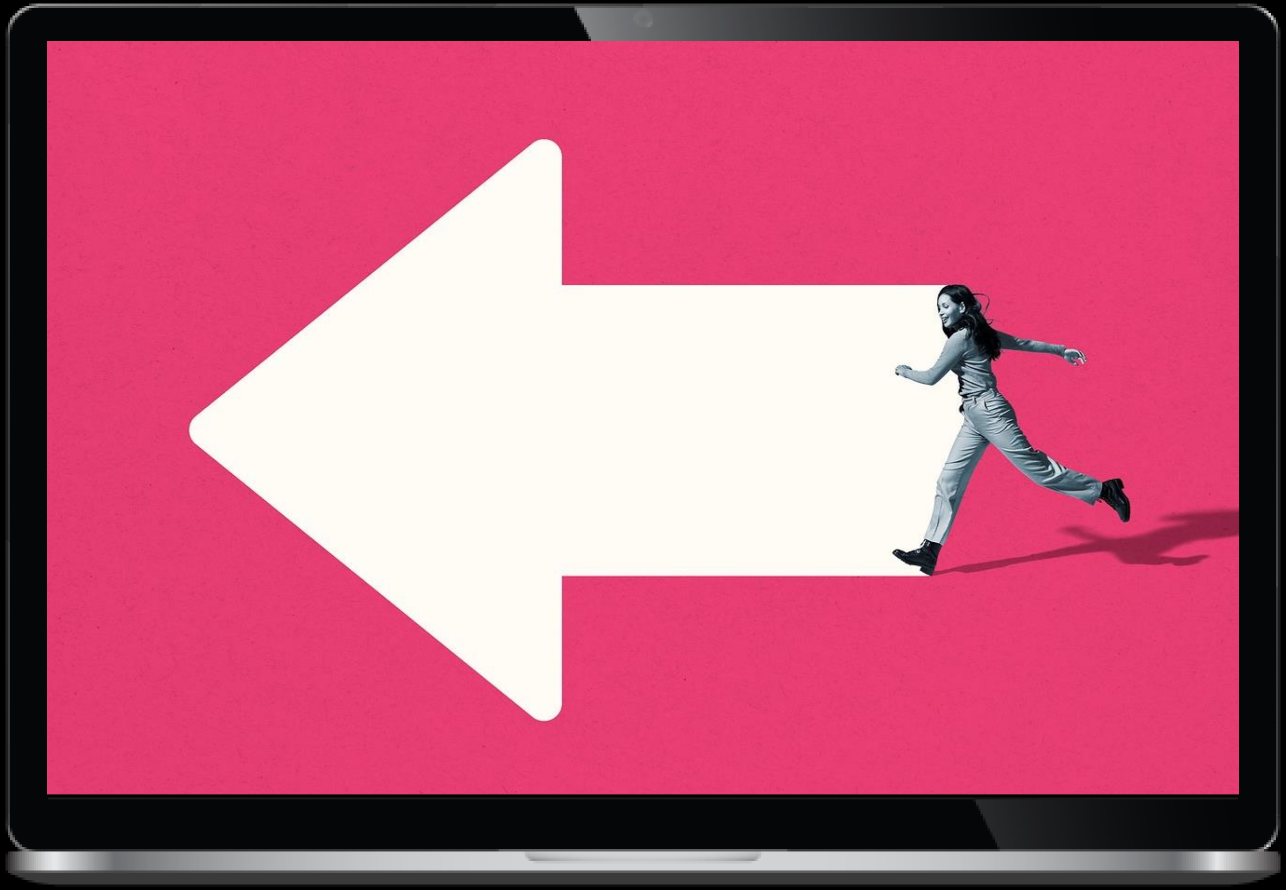
| Name | Component Version | Type | License Effective | Status |
|---|---|---|---|---|
| @foo/bar | 1.2.3 | Package | MIT | ✓ |
| @some/thing | 4.14.186 | Package | LGPL-2.1-only | ✓ |
| @another/component | 2.0.4 | Package | MIT | ✓ |
| help-me | 0.0.9 | Package | Apache-2.0 | ✓ |
| somecoolparser | 2.0.1 | Package | Python-2.0 | ✓ |
| welovecode | 4.0.0 | Package | ISC | ✓ |

Rows per page: 100 1-6 of 6

Provider/Privacy Statement | v0.9.9 from 22.06.2023 - INTERNAL DATA

# SBOM Challenges

- Common Identifiers
- Data Quality and Curating
- Required Attributes
- Obligations and Abstraction
- All Code of All Dependencies



Bildlizenz: iStock.com/DigitalVision/Klaus Vedfelt

# What’s in it for Suppliers

## Digitization

Submit the SBOMs for your apps & control units to FOSS Disclosure Portal instead of filling in a MS Word template

## CI/CD integration

Connect to FOSS Disclosure Portal API from your build pipelines

## Transparency

Full transparency and policy support enables you to align with your customer much earlier in development process

## Contributions Welcome

Disclosure Portal CLI is FOSS so that you can change it to your own needs and submit upstream for continued support
https://github.com/mercedes-benz/disclosure-cli