11-04-2024

# Deliverable D9.4
# Open Source and Licence Support Report

| | |
|---|---|
| Contractual Date: | 31-03-2024 |
| Actual Date: | 11-04-2024 |
| Grant Agreement No.: | 101100680 |
| Work Package: | WP9 |
| Task Item: | Task 2 |
| Nature of Deliverable: | R (Report) |
| Dissemination Level: | PU (Public) |
| Lead Partner: | UoB/AMRES |
| Document ID: | GN5-1-24-df5ecd |
| Authors: | Branko Marović (UoB/AMRES); Magdalena Rzaca (GÉANT Association); Milica Ristić (UoB/AMRES); Kiril Kjiroski (UKIM); Tomasz Weiss (PSNC); Marcin Wolski (PSNC) |


## Abstract

This report presents an overview of the work on intellectual property rights (IPR) and open source software (OSS) licences management within the WP9 Task 2 Open Source and Licence Support activity, including the approach; analysis services and tools; awareness raising and training; documentation and guides; the role of the Open Source Review Board; licence management workflow; intelligence on implemented licences, typical licensing situations and licensing selection in GÉANT; and recommendations, which together provide comprehensive support and guidance for software development teams.

# Table of Contents

# Table of Figures

# Executive Summary

Within the GÉANT projects, including its GN5-1 iteration, the use of third-party open source software (OSS) components is widespread, as it improves productivity for the non-core or commodity parts of development, freeing software developers to concentrate on the differentiating parts of the product, and not reinvent what already exists. However, care must be taken to ensure that the associated licences are appropriate and not infringed, and, in addition, that components do not introduce known vulnerabilities into the product, which might cause legal and/or reputational harm.

The purpose of the GN5-1 Open Source and Licence Support activity within GN5-1 Work Package 9 Operations Support, Task 2 Software Governance and Support (WP9 Task 2), is to introduce the practice of dependencies checks and licence analysis into GÉANT project software developments, as part of a wider initiative to consolidate the intellectual property rights (IPR) management of software produced in GÉANT projects. Software composition and licence analysis are activities similar to other software reviews and support provided by GÉANT Software Governance and Support, all of which are carried out upon user (i.e. software development team) request.

This report on open source and licence support presents an overview of the work on IPR and OSS licences management within the OSLS activity, including approach, analysis services and tools, awareness raising and training, documentation and guides, the role of the Open Source Review Board, licence management workflow, and intelligence on implemented licences, typical licensing situations and licensing selection in GÉANT, which together provide support and guidance for making related decisions.

It also discusses the evolution of OSS licence management in GÉANT and the changing attitude and role of software development teams towards licensing, together with the GÉANT IPR Policy reform that applies to GN5-1. The final part of the report is dedicated to recommendations relating to aspects including preparation, software composition analysis, licence selection and overall governance.

This report provides an update of the white paper *Open Source Software Licences in GN4-3 and GN5-1 GÉANT Project: Current State and Recommendations* [Wiki_OSSLWP] and summarises some of the publicly available guidelines for software developers and several operational documents that are used internally by WP9 Task 2 or shared with GÉANT software developers requesting the services of the licensing team. While adherence to the GÉANT IPR Policy is mandatory, the use of WP9 Task 2 licensing services is still voluntary.

The activities, plans and aspirations of the Open Source and Licence Support team described in the report are based on accumulated experience and newly identified needs and issues, as well as the evolving landscape and options available.

# 1 Introduction

The GÉANT Association, GÉANT projects, National Research and Education Networks (NRENs) and academic institutions can benefit from the use of open source software (OSS) in many ways, especially by reducing costs, increasing collaboration, and encouraging innovation. Other characteristics often associated with OSS are availability, flexibility, security, interoperability, reliability, transparency, and longevity.

Licence non-compliance can have severe financial implications for the GÉANT community, the GÉANT projects, and their reputation and trust. Appropriate processes around open source are important to foster international collaboration and risk management. OSS has many advantages, but its use is also linked to the fulfilment of conditions that are specified by the terms of the chosen OSS licence. Although GÉANT products and services rely on OSS under permissive licences, some also rely on copyleft ones, when developed software using such code must use compatible copyleft OSS licences or be modified so that it only depends on the code under permissive ones. Hence, awareness of OSS licences and compliance with OSS licensing conditions are crucial for the use of OSS in general and in GÉANT projects in particular.

When software is released under an OSS licence within GÉANT projects, it is made available and contributes to a wider community. The EC, many participating organisations, and developers consider that this is the best way to deal with the software intellectual property (IP) produced in the GÉANT projects. For this reason, the GÉANT IPR Policy also recommends that software should be released under permissive OSS licences whenever possible [GN_IPRPolicy].

The goal of licence governance in the GÉANT project is to ensure compliance with GÉANT's IPR Policy while respecting dependencies' licences and domain community standards. It is led by the IPR Coordinator and supported by the GN5-1 WP9 Task 2 activity Open Source and Licence Support (OSLS), also known more simply as software licensing. The OSLS team:

- Provides technical support related to licensing and use of open source, assisting project participants in managing software licences and adhering to the GÉANT IPR Policy and applicable software licences.
- Acts as a focal point for resolving open issues and assisting software teams in making decisions aligned with the GÉANT IPR Policy and the guidance provided by the IPR Coordinator on a case-by-case basis.
- Helps establish effective processes that minimise the burden on GÉANT governance and software development teams, ensuring conformance with policies.
- Helps those who prefer to invest in understanding and managing OSS licences, master the provided tools, and apply them.
- Contributes to the adoption and interpretation of and adherence to GÉANT's IPR and open source policies and provides guidance for refining these policies.
- Offers knowledge and support to solution designers, developers and skilled promoters on licences and IPR.
- Offers technical knowledge and feedback to support strategic open source software management.

The OSLS team conducts reviews and audits related to licences and IPR to determine the open source licence appropriate to the software and ensure licence compliance. It provides assistance to software development teams through the software composition analysis (SCA) service, currently based on the Mend tool [Mend_SCA].

The software licence analysis (SLA) service, built upon the SCA results, manually checks the detected libraries for IPR software compliance as necessary.

Software developers play a crucial role in OSS licensing, as they are responsible for informed licensing decisions and actions throughout the software development lifecycle, and thus also during GÉANT's SCA and SLA services. Their duties encompass selecting appropriately licensed components and other sideground IPR, choosing suitable licences for their software, understanding licence implications, ensuring compliance, and communicating these aspects to the project community. This includes informing the community about copyright, authors, modifications and dependencies. Developers contribute to collaboration, legal compliance and the open and transparent nature of OSS projects. They also effectively implement ongoing monitoring and compliance management, ensuring alignment with GÉANT's IPR Policy.

This report presents the open source and licence support provided for software developers by the OSLS team and IPR Coordinator. It is structured as follows:

- Section 2 establishes the broader context by describing the key factors and benefits of open source software and licensing. It goes on to outline the evolution of OSS licence management in GÉANT, the role of OSS in GÉANT software developments, their libraries and licences, and the GÉANT IPR Policy.
- Section 3 summarises the approach to supporting OSS in GÉANT and outlines the two key support services – software composition analysis and software licence analysis – including the SCA and SLA reviews carried out to date and some of the typical licensing situations identified by the reviews. It also covers the changing role of software developers with regard to OSS and licensing; awareness raising and training; documentation and guides; and the role of the Open Source Review Board.
- Section 4 presents an overview of licence management workflow steps, expands on the role of the software composition analysis and software licence analysis services within the workflow, considers the practicalities of complying with a selected licence, and discusses automated analysis and reporting.
- Section 5 presents a set of recommendations to ensure good practices regarding OSS licensing in GÉANT, covering preparation and support; software development; software composition analysis; software licence analysis and licence selection; licence declaration and compliance; copyright management; and overall governance.
- Section 6 offers conclusions on open source and licence support and outlines next steps and future plans.

A detailed description of the Mend SCA tool and a summary of other SCA tools and resources are provided in Appendix A; the parts of the software review feedback form that are relevant to OSLS are reproduced in Appendix B.

# 2 Open Source Software in GÉANT Software Developments

This section establishes the broader context for the report by describing the key factors and benefits of open source software and licensing. It goes on to outline the evolution of OSS licence management in GÉANT, the role of OSS in GÉANT software developments, their libraries and licences, and the GÉANT IPR Policy.

## 2.1 Significance of Open Source Software and Licensing

These are the key factors related to the use of open source software (OSS):

- The GÉANT community's work increasingly relies on OSS. Developers, National Research and Education Networks (NRENs) and GÉANT widely and increasingly use, adapt, create and endorse OSS.
- In a broader context, the ICT and R&E communities value OSS for its cost-effectiveness, transparency, collaboration, customisability, vendor independence, longevity, security, educational value, compatibility, ethical and philosophical values, accessibility and more (detailed below).
- OSS licences ensure the licensed software remains free, prevent appropriation and help avoid abandonment.
- Declaring a software licence makes it easier to select what other code and libraries can be incorporated into the project and how others can use, adapt and contribute to the software.
- Licensing considerations are critical when there is a distribution or sharing of software, as OSS licences come with specific conditions.
- Declaring a licence and licence compliance are also essential for legal reasons and software usability, ensuring better transparency and collaboration.
- Adhering to the requirements of applied licences (including those of dependencies) enhances the transparency of the software project within the wider community.

Open source software is important in various domains, including technology, research and education, business and government. It plays a crucial role in promoting affordability, transparency, collaboration, and technology innovation. It empowers individuals and organisations to take control of their software solutions, adapt them to their needs, and contribute to a global community of developers and users. The benefits of using and producing OSS include:

1. **Cost-effectiveness** – Open source software is often free to use, significantly reducing software acquisition and licensing costs for individuals, businesses and organisations. This cost-effectiveness is especially critical for smaller businesses, educational institutions and governments with budget constraints.
2. **Transparency** – Open source software is built on open and transparent development processes. Anyone can review the source code to understand how the software works, enhancing trust, reliability and security. Although transparency does not guarantee that the software used will be flawless, it greatly supports the detection and resolution of vulnerabilities and other bugs, and is particularly important for software used in critical applications, such as cybersecurity and healthcare.
3. **Community collaboration** – Open source projects typically have large and diverse communities of developers and users who collaborate to improve the software. This collaborative approach results in

rapid bug fixes, updates and feature enhancements. It also fosters innovation and the sharing of knowledge.

4. **Customisation** – Users of open source software have the freedom to modify and customise the code to suit their specific needs. This flexibility allows businesses and individuals to adapt software to their unique requirements, giving them a competitive edge.
5. **Vendor independence** – With proprietary software, users are often locked into a single vendor's ecosystem. Open source software reduces vendor lock-in, as users have access to the source code and can switch service providers or modify the software as needed.
6. **Longevity** – Proprietary software may be discontinued by the vendor, leaving users without support or updates. Open source software tends to have longer lifespans, as the community can take over maintenance and development if the original project loses momentum.
7. **Security** – Open source software is not immune to vulnerabilities and benefits from transparency which enables a global community to audit the code for security flaws and swiftly address any issues found. In contrast, the security of proprietary software relies solely on the vendor's resources and priorities. However, robust security requires adherence to proper development practices, thorough code audits, a controlled release process, and prompt updates by downstream developers and users. Without these measures, vulnerabilities become more accessible for malicious actors to discover and exploit.
8. **Education and learning** – Open source software encourages learning and skill development. Students and aspiring developers can study, modify, and contribute to open source projects, gaining practical experience and exposure to real-world software development.
9. **Compatibility** – Open standards and open source software often go hand in hand, promoting compatibility and interoperability between different software and systems and reducing barriers to data exchange and collaboration.
10. **Ethical and philosophical values** – The open source movement is rooted in values such as transparency, collaboration, and the idea that software should be a public good. Many individuals and organisations choose open source software to align with these values and principles.
11. **Global accessibility** – Open source software is accessible to users worldwide, regardless of location or economic status. This accessibility promotes digital inclusion and levels the playing field for all users.

Despite the success and benefits of OSS, it is still difficult to scale and sustain open source projects unless they are supported by at least one strong proponent or a large community.

OSS licences keep OSS alive by ensuring that key tenants are upheld and freedoms guaranteed. However, they also come with strict conditions that include free distribution, access to source code, permission to create modifications and derived works, and non-discrimination against fields of application, individuals, or groups. Unlike the Creative Commons CC BY-ND and CC BY-NC licences, an OSS licence must allow modification or commercial use to be considered truly open. Many OSS licences also require that notes about previous contributions are preserved.

Licence compliance is important not only for better collaboration but also for legal reasons and the possibility of legal sanctions. Licensing considerations become very important when software is shared with other users.

OSS without identifiable licence terms can be problematic because, in many jurisdictions, creative works (including code) by default fall under exclusive copyright. Another problem is that it is not that common to assign a licence to a project developed under OSS. GitHub only introduced the requirement to assign licences to OSS projects a few years ago.

The OSS landscape is further complicated by the occasional use of dual- or multi-licensed projects offering several open or open and proprietary licences. These, along with source-available and "fauxpen" licences, are

detailed in *OSS licences and licence selection* [Wiki OSSL&LS]. Source-available and "fauxpen" (a term combining "faux" and "open") are non-OSS restrictive proprietary licences often presented or perceived as similar to OSS.

Business models based on open source software include professional support services, documentation, software as a service (SaaS), training and certification programmes, and the open core model. Open core furthers the pure dual-licensing model by offering additional proprietary extensions, features or content, often branded as "enterprise version". Market forces eventually equalise total cost of ownership (TCO) between mainstream proprietary products and comparable OSS. Additionally, proprietary software is often superior in terms of the quality of documentation provided, expertise involved and support offered.

However, the unique and highly specialised services provided by the GÉANT project, which often leverage novel or cutting-edge technology, tend to necessitate custom software solutions. Its community, primarily from research and education organisations, is predisposed towards and accustomed to using OSS, often viewing it as an avenue to fostering innovation and enhancing their skills. The pooling of NRENs' expertise and manpower may also bring additional benefits of OSS unmatched by commercial products, especially in widespread system implementations.

Section 5 and [Wiki OSSL&LS] recommend careful selection of well-maintained and documented OSS using quality and trustworthiness checklists. Software teams are advised to examine primary contributors and backers of key components that are under permissive licences to anticipate potential switches to "fauxpen" and other proprietary licences.

## 2.2 Evolution of OSS Licence Management in the GÉANT Project

OSS licence management was initiated in the previous iteration of the GÉANT project, GN4-3, under the term Software Licence Management as a part of wider WP9 Task 2 Software Governance and Support activity. During that project phase, significant efforts were made in the areas of software licences and IPR, as well as to establish effective communication channels with the software development teams and to increase software developers' awareness of OSS licences and the importance of complying with them. In addition to work focused on updating the GÉANT IPR Policy for the project (which was prepared during GN4-3 and applies to GN5-1), led by the IPR Coordinator with the cooperation of Work Package Leaders, and, in particular, WP9 Task 2 involvement, the software composition analysis (SCA) tool was introduced to support licence compliance (see Sections 4.2 and A.1 for further detail about the SCA service and tool respectively).

The part of the GN4-3 WP9 Task 2 team responsible for the SCA tool worked intensively with the IPR Coordinator on aligning the licence reviews with the GÉANT IPR Policy and with other software review services, adapting existing operational workflows to include the third-party licences analysis service. It also provided general support to the IPR Coordinator for the development of IPR management criteria, practices, tools, and guidelines. The work on common best practices also included a practice for managing sideground IPR that is aimed at achieving compliance with the GÉANT IPR Policy and compatibility of the project's software licence with third-party components [SideIPR]. It therefore applies to OSS and proprietary licensed projects that use external libraries, components, source code, frameworks, data, designs or other IPR provided by third parties.

This effort has been continued in GN5-1, with an increased emphasis on actual licensing of software projects. The purpose of the GN5-1 Open Source and Licence Support activity is to introduce the practice of licence analysis and dependencies checks into GÉANT software projects, as part of a wider initiative to consolidate the IPR management of software produced in GÉANT projects. Software composition and licence analysis are activities similar to other software reviews and support provided by GÉANT Software Governance and Support. Specifically, it aims to:

- Encourage project teams to proactively manage IPR and software licensing issues.

- Evaluate licences used in software projects and the issues associated with them.
- Support software projects in GÉANT with licence analysis, licence selection, and licence management.
- Assist the IPR Coordinator in the governance of IPR by providing information about the general distribution of licences for libraries in use and common issues experienced in managing licences for software projects.
- Prepare educational materials and inform software developers about OSS licences, licence management and software compliance.
- Assist project teams in licence selection and achieving compliance with selected licences.
- Provide feedback on the implementation and enforcement of the GÉANT IPR Policy and suggest possible improvements.
- Determine useful data presentation methods and analyses that could be done by using the SCA and other related software tools.
- Assess the SCA and licence compatibility analysis tools that could be used in future work.

The accumulated and documented knowledge and established software licence management system provide a robust foundation for monitoring, verifying, and optimising OSS licences used in GÉANT software development projects and compliance with selected licences. Ongoing efforts focus on refinement, user training, and the incorporation of advanced features to further streamline licence management processes.

## 2.3 OSS in GÉANT Software Developments

The work of software development teams in general and within the GÉANT project in particular strongly depends on OSS. Most software made available to NRENs or the wider public is OSS, or, more precisely, its source code is made available to the general public but sometimes without declaring its licence. Only the software that is internally used to access GÉANT services is sometimes kept proprietary.

No catalogue contains all the software that was produced during different GÉANT project iterations. A few years ago the GÉANT Software Catalogue [SC] was introduced to track the produced software; a feature was added to it to track project licences only recently. Virtually all software developed within the GÉANT project resides in source code repositories, and much of it is considered to be OSS. Many components still lack an assigned or documented OSS licence. However, this is a situation where no one else can use, copy, distribute or modify that work without risking litigation and copyright infringement unless there is a licence to specify otherwise, or authors explicitly give their permission for this to users who directly request it.

A typical project may contain many hundreds or thousands of such components, and before releasing a public version of software, a check is recommended to ensure that the developers have the necessary rights to use these components as intended, and that any software vulnerabilities associated with them have been identified and remediated. This check is mandatory for passing the final gate of the Product Lifecycle Management (PLM) process and moving software into production. However, the process by which this is achieved is manual and prone to errors or omissions. It cannot be expected to successfully identify all components and their licences, associated issues and software vulnerabilities. As a result, GÉANT may be subject to legal action in the event of a licence breach, and the release of software with security vulnerabilities may damage its reputation.

To help address this, software-automation tools that can improve the rigour of licence selection and reduce the potential risks were examined. The Mend (formerly WhiteSource) SCA tool [Mend_SCA] was identified by a small team as one of the best, and a suitable licence was purchased. Still, the use of Mend does not ensure fully accurate component or licence detection, not to mention identification of a software licence that is most suitable for a software project, but it does improve the due diligence process around OSS.

Defining and implementing software licences for software projects should be integrated into the GÉANT PLM process, as this must be done before a service enters production at the latest; the introduction of licence management into the PLM process is ongoing. However, it is better to define the appropriate licence before much of the development has taken place, but after the main dependencies and their licences have been determined.

Those considerations were taken into account in Article 13.1.3 of the IPR Policy: *Before any OSS created during the Project is subjected to Public Disclosure, it should be submitted for a review including licence compliance analysis and an additional vulnerability test performed with the Software Composition Analysis (SCA) tool* [GN_IPRPolicy].

Article 13.1.1 also highlights the supporting role of the IPR Coordinator: *Task Leaders, Work Package Leaders, as well as Participants and Partners, are encouraged to contact the IPR Coordinator as early as possible to establish which OSS licence will be best suited to the software generated during the Project and its aims*.

Also, copyright should be declared and attributed to the appropriate GÉANT project, as stated in Article 14 *IP Attribution and Information about Funding*.

However, recognition of the IPR Policy and related responsibilities among the development teams is still suboptimal, despite efforts by the IPR Coordinator and the OSLS team to inform and raise awareness. One of the key reasons for this is that many software projects were initiated years ago and tend to continue operating as they are used to, without properly addressing licensing. Also, software developers are engaged or contracted to design a solution or implement some features and often consider IP and licensing issues to be outside their area of responsibility. They are not aware of IPR's existence, or that they should declare GÉANT's copyright for the products of their work; simply, this information is not a part of their onboarding, or is small collateral in their project onboarding and domain familiarisation package. Hence, infoshares and training sessions dedicated to those topics are essential for creating the necessary IPR awareness.

## 2.4 Libraries and Licences in GÉANT Project Software Developments

Many software products comprise a large number of libraries, and Mend reports that the number of libraries can reach several hundred, due to transitive dependencies. This number does not change significantly over time unless major refactoring takes place. It can also be affected by the environment for which the dependencies are resolved, e.g., Linux, Windows, or Docker. Reported differences between runtime platforms are now becoming smaller as Mend strives to refine the boundary between user OS and platform libraries. If this number is large, the risk of security vulnerabilities or licence incompatibility is higher.

Another important metric is the number of different licence types, which can be up to a few dozen and is determined by the number of libraries that use the same licences. Removing some libraries from the product can, therefore, significantly reduce the number of transitive dependencies and the total number of libraries without affecting the number of applied licences. From the point of view of IPR management, the fewer licences the better, as this makes it easier to select licences and maintain licence compatibility.

Most libraries used by GÉANT project software projects have a permissive licence. They typically cover between 65% and 97% of the project libraries (see Figure 2.1). This is in line with the GÉANT IPR Policy's preference for permissive licences for software projects.

The OSLS team has compiled comprehensive information about OSS licences, some of which is also available via Mend, the tool used for SCA (described in Section A.1). However, there is a limited set of licences that are frequently used in the GÉANT project or are common sources of compatibility issues.

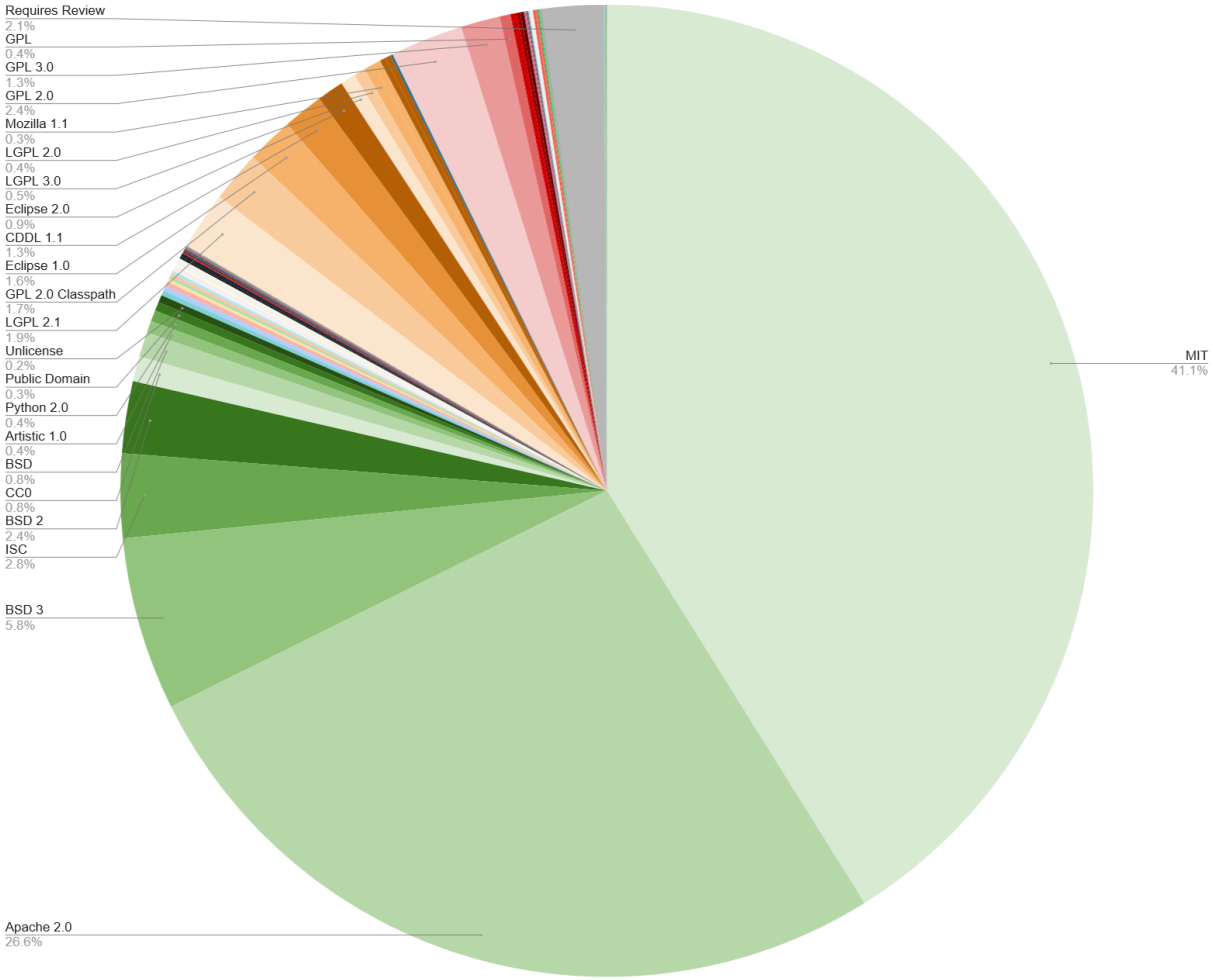


Figure 2.1: Overall distribution of component licences in GÉANT project software projects scanned with Mend to date

As can be seen from Figure 2.1, more than 80% of dependencies in GÉANT project software use permissive licences such as MIT, Apache, BSD, ISC, Artistic and Python, or are in the public domain. Following in frequency are weak copyleft or similar non-viral licences such as LGPL, Eclipse, GPL Classpath, CDDL and Mozilla. These should not be of concern in product licensing unless the primary task involves modifying these external libraries, which is seldom the case. The third group comprises strong copyleft licences such as GPL and AGPL. The smallest group consists of projects that require review, do not have a specified licence, or have a suspected licence. The rarest occurrences are a few instances of commercial or proprietary licences among the 9,298 detected uses of libraries in distinct projects. At present, 90 licences are used by 8,126 libraries.

Figure 2.2 presents an orientational diagram describing the relationships and compatibility of the most frequently used licences. Please note that there are two distinct interpretations of licence compatibility. A less restrictive, more commonly used and symmetrical type of compatibility indicates that components with two distinct licences can be used in the same project, which may be achieved by relicensing one or both of them or by selecting a third licence for the encompassing product. A more restrictive and direct, yet asymmetrical, interpretation determines whether a component under one licence may be used in software under another licence. Although the first interpretation is dependent on the second, various types of “use” by the produced software exist and sometimes can be altered by modifying the system architecture to allow the integration of a problematic component without needing to change the licence of the created software.

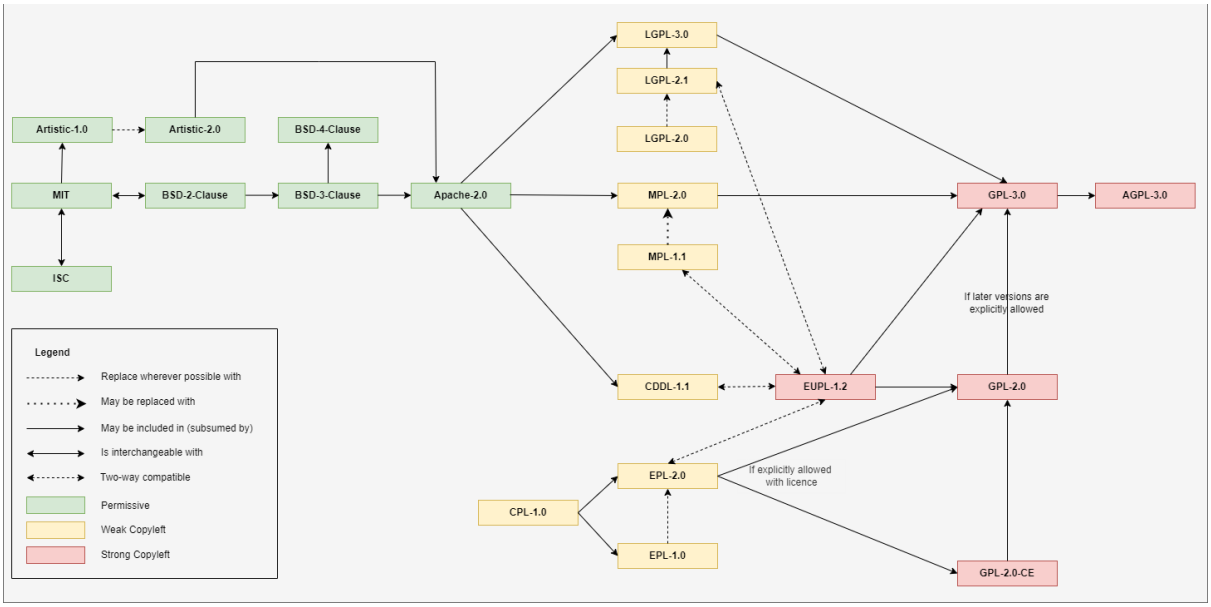


Figure 2.2: Relationships between OSS licences frequently used in GÉANT projects

OSS licences are described in several documents produced by the licensing team. For additional details, please refer to the following guides: *Reference information about OSS licences and tools* [Wiki OSSL RefInfo], *OSS licences and licence selection* [Wiki OSSL&LS] and *Important licences for licence selection* [Wiki ImportantLicences].

## 2.5 GÉANT IPR Policy

The GÉANT project is developing software products based on the use of OSS components that may be licensed under a variety of terms, and have been developed by a range of third-party organisations and individuals. In 2019, before GN4-3 started, there was no process or tool in place to identify OSS licences and verify that their requirements were met. A systematic addressing of software based on OSS licences, analysis of licence requirements and potential liabilities, and preparatory work on the GÉANT IPR Policy was started in GN4-3. Also, before the introduction of the software composition analysis tool, it was not possible to check which OSS licences were being used in the code provided for review, and ensure that all licence requirements were met.

The fact is that OSS is governed by its licensing terms, which, in most cases, include strict contractual licensing restrictions. This was the reason for introducing the SCA tool, updating the IPR Policy, and introducing more best practices to the GÉANT project's software development and training.

During GN4-3, an updated approach to licences and the IPR Policy for the GÉANT project was developed [Wiki OSSL&LS] and has been maintained in GN5-1.

After extensive consultations, the IPR Policy was voted on with resolution GA(22)037 and unanimously approved with the GA decision GA27-D05 at the GA meeting on 13 June 2022 in Trieste [GA].

The work on the updated policy took more than two years and all the details of the process can be found on the GÉANT project's wiki [IPRUpdate]. The new policy, which has been binding from the moment of its approval by the General Assembly and as of the start of GN5-1 in January 2023, can be found online at [GN IPRPolicy]. In addition, an infoshare on the IPR Policy was held in November 2022 [InfoSharePolicy], and a session was dedicated to OSS at the Project Symposium in December 2023.

The GÉANT IPR Policy applies to IP generated within the GÉANT project, including open source software. It also provides related recommendations and rules. The IPR Policy seeks to establish a framework for the intellectual property (IP) generated by the GÉANT project. It applies to all project participants of the GN5-*n* project and any other EC-funded GÉANT projects and provides practical and useful guidance in the area of IPR. Most importantly, the IPR Policy aims to establish a cooperation modus operandi and proper protection as well as fair use with regard to any IP created by GÉANT projects. The IPR Policy also aims to apply the principles of findability, accessibility, interoperability and reusability (FAIR) in the use of the project IP.

To summarise the IPR Policy:

- **All OSS licences** [OSI Licences] **are allowed**.
- The IPR Policy strongly **recommends the selection of permissive licences**.
- Copyleft licences (weak, strong or network protective) can be applied as necessary, in consultation with the IPR Coordinator.
- The IPR Coordinator provides the final recommendations and maintains the GÉANT IP Register.

The WP9 Task 2 software licensing team provides related services, support and guidance. Related guides developed by the team are listed in Section 3.6 Documentation and Guides while training and infoshare events and corresponding presentations are listed in Section 3.5 Awareness Raising and Training.

What is important from a software development perspective is that there is a software composition analysis (SCA) tool and service that allow a software scan to check and verify the licences of used components and determine which licence shall be used. This analysis is followed by support provided through the software licence analysis (SLA) service, which should result in a decision on the appropriate software licence and achieving compliance with it.

Failure to comply with OSS licence terms can have significant legal and monetary consequences, hence due diligence is required. The IPR Policy emphasises the importance of IP protection, introduces the GÉANT IP Register where project results will be documented, and highlights the significance and necessity of having the code scanned with an SCA tool to ensure licence compliance and compatibility. It also highlights the role of the IPR Coordinator in supporting project participants with the licence selection process.

Possible future directions are for further development of the IPR Policy and IP governance, including precise direct guidelines on licences that are most suitable or are to be recommended in specific situations, such as when to opt for a permissive licence, EUPL, or, for compatibility or relicensing-avoidance reasons, select a copyleft licence. It may also elaborate more specifically other IPR that is used in or by software, is produced by it or is otherwise related to it. The policy could also provide additional details on how the GÉANT IP Register is operated, or what software and licence metadata is to be tracked in the GÉANT IP Register, Software Catalogue, or software project repositories.

# 3 OSS Licensing Services and Support in the GÉANT Project

The need to introduce comprehensive support for software IPR was clearly expressed by the GÉANT project teams that participated in a survey conducted in 2019 to identify common best practices [BP]. IPR management at that time was rated negatively by most respondents [GN4-3_D9.2]. They mentioned difficulties related to IPR and dependencies' management, such as understanding and interpretation of imported licences, as the previous IPR Policy (from 2011 and binding in 2019) was thought to be not very helpful. When the IPR Coordinator took up her position in 2019, updating the IPR Policy and collaborating more closely with software teams to identify the main issues and provide guidance were her top priorities. A thorough investigation of the software composition analysis tools took place in 2019, and the best option at the time was chosen and introduced later in 2020.

One of the key findings from the survey was that GÉANT project teams identified the provision of support for managing software IPR as essential. They needed a comprehensive approach that would include a versatile tool for licence compliance checks, support for the decision-making process (e.g., licence selection), and a constantly updated knowledge base about IPR, open source software (OSS) licences, and related processes.

Building on the foundational work undertaken in GN4-3, the open source software licence management and support activities in GÉANT now span various aspects, including conducting reviews, running the services, providing documentation, fostering collaboration, performing integration and liaising with other related initiatives, demonstrating a comprehensive approach towards effective licence management within the GÉANT environment.

This section summarises the approach to supporting OSS in the GÉANT project and outlines the two key support services – software composition analysis and software licence analysis – including the SCA and SLA reviews carried out to date and some of the typical licensing situations identified by the reviews. It also covers the changing role of software developers with regard to OSS and licensing; awareness raising and training; documentation and guides; and the role of the Open Source Review Board, which was established to support the WP9 Task 2 Open Source and Licence Support (OSLS) team.

## 3.1 Approach to Supporting Open Source Software

Where services and solutions are created in the GÉANT project, it is important to deal effectively with OSS to ensure compliance with licensing requirements, minimise legal and financial risks, and reap the benefits that OSS can offer. To deal effectively with OSS, the GÉANT project follows, and recommends, the following approach:

1. **Develop a clear policy** that governs the use and distribution of OSS. This policy should consider licensing requirements, copyright and trademark laws, and ethical considerations. GÉANT created its IPR Policy from 2020 to 2022. It was approved in June 2022 and became effective in 2023 [GN_IPRPolicy].
2. **Conduct due diligence** to ensure that OSS usage complies with licensing requirements and is free from potential legal or financial risks. This may include reviewing the licence agreement and checking for known vulnerabilities or security issues. As GÉANT integrates OSS into its services, products, and solutions, it offers software-related projects within GÉANT the Mend tool (a software composition analysis and vulnerable components detection tool [Mend_SCA]) through the software composition analysis service provided by WP9 Task 2.

3. **Provide training** to participants on the use of OSS and the requirements of open source licences. This can help ensure that service and product managers, practitioners, and developers are aware of the legal and ethical considerations when using OSS. The first GÉANT OSS licensing training was held in February 2022 [OSLC Training]; the second training took place in April 2023 [IntroOSLC Training].
4. **Provide support** for OSS by providing access to technical resources, expertise, and support staff. This support can help ensure that software is installed, configured, and maintained properly. This is the responsibility of the IPR Coordinator and WP9 Task 2, who work closely together to identify gaps and address them.
5. **Encourage the use of OSS** by offering resources to GÉANT project participants. This can include organising workshops and events to showcase the benefits of OSS and provide practical experience. In the GÉANT project, OSS is already extensively used in most software projects because it is ubiquitous and often a necessity. The adoption of the GÉANT IPR Policy officially endorsed this practice. In addition, there is a wider discussion about the use of open source and its associated benefits.
6. **Promote collaboration** by encouraging participants to share their work and contribute to open source projects. This can lead to increased visibility and recognition for the institution and its researchers. This is practised in the GÉANT project and is another reason why due diligence and compliance are necessary and important.
7. **Contribute to the open source community** by providing software, bug fixes, improvements, documentation and OSS-related practices, contributing to projects, participating in discussions, and spreading the word about the use of OSS tools. This can help build relationships with other projects, providers, and organisations, as well as increase the visibility and reputation of the GÉANT project.

## 3.2 Support Services: SCA and SLA

In GN5-1, the Open Source and Licence Support (OSLS) team provides technical and implementation support on open source software and licence management through two services:

- **Software composition analysis (SCA)** – Technical and practical assistance for software development teams with managing software components and their software licences. The service assists development teams with managing software components and licences through the SCA tool Mend, providing insights into third-party libraries, licences, and security vulnerabilities. The SCA team helps software developers by setting up a project in Mend, and by providing insight into the external libraries. Mend is used to identify third-party components and obtain information about their licences and security vulnerabilities. The SCA service is recommended for teams that want a one-off analysis of their software or expect regular feedback on risks related to IPR infringement and associated security vulnerabilities in third-party libraries.
- **Software licence analysis (SLA)** – Assistance to software teams in aligning their project and licensing decisions with the GÉANT IPR Policy and the guidance provided by the IPR Coordinator. The service provides deeper insights into the third-party libraries in the software project and their licences, which is necessary for choosing or adhering to the project's software licence. Based on the outcome, the development team can refine the project's licensing approach, select the appropriate software licence, or adjust software dependencies. This service is recommended for teams wanting to verify their licensing decisions, compliance, third-party licences, or the effects of changes to their software.

These services complement other software review services provided by WP9 Task 2 Software Governance and Support, namely SonarQube Setup Assistance and Extended Source Code Review [Wiki SWReviews]. Through SCA and SLA services, the licensing team ensures the handling of key licensing concerns by:

- Assessing the situation with licences of components and prior IP.
- Selecting an open source licence for the software project's needs.

- Making sure the selected licence is compatible with the components' licences.
- Ensuring compliance with the chosen licence.

The OSLS team helps GÉANT software teams address IPR and licensing issues by implementing robust processes for managing dependencies and licences and achieving compliance with the GÉANT IPR Policy. It provides teams with mediated, managed access to expert tools for analysing and managing open source components and their licences, but also direct access to those who prefer to invest effort in understanding OSS licences themselves, master the tools provided, and apply them on their own. The OSLS has worked with many GÉANT software development teams to assess their licensing situations and decisions, with resulting recommendations to support reliable and effective IPR management, in line with the GÉANT IPR Policy.

The OSLS also provides knowledge and support regarding licences and IPR to solution designers, developers and skilled promoters. Additionally, it can act as a bridge to access appropriate legal support for teams that prefer a single technically oriented point of contact for licensing and IPR.

GÉANT development and maintenance teams can contact the OSLS through the GÉANT project Slack channel or email [Contact]. SCA and SLA services are requested by submitting a software review request to the GÉANT Jira Software Tools Help Desk [HelpDesk], which also serves to track the progress of the work on them. Several iterations of analysis and licence and dependency adjustments may be required to reach satisfactory IPR status. The IPR Coordinator can be reached when assistance with licensing decisions is needed [IPRSupport].

Practical measures to support licence compliance and IPR management include integrating them into software governance best practices, incorporating considerations within Product Lifecycle Management (PLM)-related procedures and gates, tracking software licences within the GÉANT Software Catalogue, integrating SCA into continuous integration / continuous delivery (CI/CD) toolchains and identifying, testing and evaluating new tools and functionalities that can support SCA and SLA services.

The guides developed by OSLS assist with licensing and using SCA and SLA services. These include the comprehensive guides *OSS licences and licence selection* [Wiki_OSSL&LS] and *Software licence selection and management in GÉANT* [SLS&MG], and the more technical guides published in the Software Development Support Knowledge Base [KB]. Since the SLA service requires the software development team's involvement in licence selection, it is recommended that they read the *OSS licences and licence selection* guide before requesting the service. It also helps with interpreting the software composition analysis results. However, those who are already generally familiar with OSS licences or simply want to get summaries of licences that are frequently present in GÉANT software projects or learn about typical licence compatibility problems may go directly to the *Important licences for licence selection* guide instead [Wiki_ImportantLicences]. These guides will be regularly updated and expanded to reflect evolving experiences and needs in licence compliance and IPR management. The OSLS team also contributes, together with the IPR Coordinator and the GÉANT Learning and Development (GLAD) team, to ongoing training and awareness campaigns on licences and IPR.

SCA and SLA present a valuable opportunity to elevate and align a software project with both GÉANT's and external expectations, encompassing licensing and policies. The analysis, selection and validation of software licences can greatly enhance the projects and bolster their credibility within the GÉANT community and beyond.

Engaging in software licensing offers a chance to meticulously evaluate the project's components, review their licences and consider aspects related to authorship, ownership, external relations and expectations, and associated documentation artefacts. This concerted effort contributes to standardising various projects in these respects. Licensing reviews engage individuals who were not the original developers to assess and validate the software project, injecting a significant impetus for its developers to critically evaluate and consolidate their work.

Furthermore, this activity entails registering and publishing software using GÉANT's internal software development tools and aligning them with established practices and expectations within GÉANT. The successful completion of licensing and the formalisation of the licence stand as positive indicators for the project within GÉANT. This holds particular significance for smaller and relatively autonomous developments, such as those undertaken within the GÉANT project incubators, as it can enhance visibility and overall improvement in the practices and visibility of the originating activity. Moreover, addressing issues through licensing analysis and the resultant reports and decisions yield valuable insights for assessing software solutions and the services based on them during their evaluation at GÉANT Product Lifecycle Management (PLM) gates [PLM].

The performed analyses, when conducted for a module that is an add-on for an externally developed open source platform, may also benefit the broader community of the software platform the development team used or contributed to by assessing the overall status of its licensing and the security of its components. This is a side effect of the analysis of software produced by GÉANT's software development teams, as it transitively includes an analysis of involved components and licences.

### 3.2.1 SCA and SLA Reviews in GN5-1 to Date

An overview of SCA and SLA reviews and related activities carried out since the beginning of GN5-1 is shown below:

- Software composition analysis (Mend) reviews)
  - Conducted repeated review of Network Management as a Service (NMaaS) 1.5.2.
  - Conducted repeated review of Vulnerability Assessment as a Service (VAaaS), version SCA_2023, alongside other software governance reviews.
  - Conducted an initial scan of FileSender 3.0.beta5, with pending analysis scope clarification.
  - Reviewed the eduGAIN Reporting ecosystem (as of 12 March 2024) after addressing concerns related to software naming and branding, packaging into software repositories, and registration in the GÉANT Software Catalogue.
  - First scan for User Profile Page plugin for Shibboleth (SHBPRFL 0.8.0); the Mend scan of the plugin was provided after several attempts to widen its scope to entire Shibboleth platform.
  - Completed the first review of Maat (formerly Inventory3) 0.9.1 and rescanned it after it was updated.
  - Completed the first review of InAcademia plugin 1.0 for a major e-commerce platform.
  - Paused an SCA request for a repeat review of the GÉANT Software Catalogue 1.10.0 after consulting on its licensing status; the prior SCA was conducted in 2022; awaiting a stable release.
- Software licence analysis reviews
  - Examined licences of components in three projects (Firewall on Demand (FoD), the eduGAIN Reporting Tool, and TimeMap) scanned with WhiteSource/Mend during GN4-3 to assess licensing and copyright status and discussed licences with their developers in preparation for SLA requests.
  - Completed analysis for InAcademia plugin 1.0.
  - Reviewing modifications to Maat 0.9.1 by developers after receiving comments from SLA.
  - eduGAIN Reporting ecosystem: review in progress.
  - User Profile Page plugin for Shibboleth (SHBPRFL): review in progress.
  - Awaiting SCA for GÉANT Software Catalogue.
- Other
  - Encouraging development teams to plan for SLA requests alongside SCA.

- Refined the SCA process and client interaction based on experiences with the eduGAIN Reporting ecosystem and User Profile Page plugin for Shibboleth.
- Moving towards a "shifting left" approach to the SLA service, delegating certain tasks to software developers.
- Promoting OSLS with individual WP5 Trust & Identity Services Evolution and Delivery developments, including its T&I Incubator, to stimulate requests for SCA and SLA.
- Introduced a new multi-phase feedback form used for all WP9 Task 2 reviews, now utilised by both SCA and SLA, replacing the previous SCA feedback survey used in GN4-3. The complete form is available at [WP9T2_ReviewFB]; the parts specific to OSLS are reproduced in Appendix B.

## 3.3 Typical Licensing Situations

As previously stated, the GÉANT Association and the GÉANT project support wider community collaboration, promote OSS projects, and aim to ensure that software developed within the GÉANT project is freely available for reuse by research and educational institutions. This is best achieved when GÉANT software projects use permissive open source licences such as MIT, BSD-based licences, or Apache License 2.0. These licences guarantee the freedom to use, modify, and redistribute the code. Besides these, the Open Source Initiative (OSI) has approved many other OSS licences. These include strong copyleft licences such as the GPL, which require that all modifications or redistributions be licensed under the same or a compatible licence. Such licences restrict the ability to reuse the code, as software under a strong copyleft licence cannot be incorporated into software under permissive licences.

To ensure that all produced intellectual property (IP) is under permissive open source licences, software dependencies need to be carefully checked and curated. Sometimes this will require additional work as components using non-permissive licences will need to be removed (if they are used for non-critical functions), replaced with permissive alternatives, or modified for internally developed solutions. However, such remediation may not be possible due to background IP, or if a component that implements critical functionality is only available under a strong copyleft licence. In this case, a strong copyleft licence can only be approved by the GÉANT IPR Coordinator. Even if a strong copyleft licence is approved, not all licence compatibility issues are resolved, as different copyleft licences used are often incompatible with each other. This even applies to different versions of GPL and LGPL licences.

More details on licences and their requirements can be found in *OSS licences and licence selection* [Wiki_OSSL&LS], Appendix A of which summarises the basic characteristics and additional features of frequently used software licences, and *Important licences for licence selection* [Wiki_ImportantLicences]. This information is useful when selecting a software licence, but also when analysing compatibility between different licences.

To ensure licence compliance and compatibility, each project should be scanned with the GÉANT-recommended software composition analysis tool (currently Mend), as this is a prerequisite for an informed licence selection.

Based on a number of SCA scans performed by the OSLS team and a deeper analysis of several software projects, some typical situations can be identified (any recommendations arising are also included in Section 5):

- Some products have been carefully managed or audited in terms of IPR and component licences, and have licences of dependencies that are suitable for a permissive licence, as recommended in the GÉANT IPR Policy.
- The most serious practical problem observed in some of the assessed projects arises from mixing GPL 2.0-only and GPL 3.0 licensed components since GPL 2.0-only cannot be subsumed by GPL 3.0. Similarly, a mix of components under Apache 2.0 and GPL 2.0-only or LGPL 2.0/2.1 is problematic as the code under Apache 2.0 can be used in projects under with GPL 3.0 but not together with the other mentioned

licences. Such situations necessitate removing or replacing some dependencies. For libraries under LGPL 2.1 this can be resolved by relicensing them to LGPL 3.0 upon obtaining permission from copyright holders.

- Other projects have many components that are under a permissive licence (MIT, BSD or Apache), but also some under copyleft or other more restrictive licences. These projects often use MySQL which implies the use of GPL 2, GPL 2+, GPL 3 or GPL 3+ for the whole software project, or requires switching to another permissively licensed database. Other potentially problematic components include MongoDB, which was available under AGPL 3.0, but has been under the proprietary Server Side Public License (SSPL) since 2018, and Elasticsearch, which moved from Apache 2.0 to SSPL and "fauxpen" source-available Elastic License 2.0 in 2021.
- There are also situations that require additional adaptation and effort but not significant refactoring. For example, projects that rely on Apache-licensed components and prefer to apply the Apache licence must be licensed under GPL 3.0 or AGPL 3.0 even when they have just one such dependency. However, libraries with Mozilla 2.0 or Eclipse 2.0 licences can be integrated into projects under Apache 2.0, GPL 3.0 and AGPL 3.0 if some reconciliatory steps are taken. Developers are rarely aware of these requirements and assume that, since Mozilla 2.0 and Eclipse 2.0 are permissive licences, they have no further obligations with components using them.
- Some projects use obsolete or vulnerable libraries. These need to be replaced.
- Code dependencies can be introduced using an automated testing framework such as Selenium. They may include different components depending on the platform used for testing (e.g., Selenium WebDriver or MS testing framework). Most of these are under Apache 2.0, Unlicense, or BSD. However, this should not affect the product licence.
- Even if the licence for the product is easy to choose or the desired licence is easy to adapt to, licence selection may be complicated by the product's participation in a broader product portfolio of a larger service brand. In such cases, it would be better to license all or at least most products uniformly, as this not only simplifies the situation for users but also facilitates subsequent recombination, repackaging or sharing of the code, as needed. This means that several products need to be analysed and, if possible, put under the same licence.
- Some components or their licences may not be properly recognised by the SCA tool. This requires a manual check, which can be very labour-intensive.
- Mend often reports GPL 2+ licences as GPL 2 (or worse, as GPL with no version information), which makes a big difference in terms of licence compatibility. GPL 2 and GPL 3 licences of components are not compatible with each other, while GPL 2+ and GPL 3 are. In general, GPL 3 and LGPL 3 are more compatible with other licence types (especially Apache 2.0) than GPL 2 and LGPL 2.1. Therefore, a component under GPL 2 only (without "or later") may severely limit the use of other components and the choice of product licence.
- A project may contain graphical or UI resources such as images, vector graphics, JavaScript code or preset GUI layouts. The problem with these resources is that it can be very hard to trace them back to their source unless they are annotated in the repository, or by using embedded metadata or comments. Internally created resources are not a problem, but resources that came with a licence or with a software component (but needed to be placed separately) can be difficult to trace back to their source later, as they are often placed separately from the code and reside in a folder dedicated to that type of resource without any reference to their source or the package they came with. In this case, an SCA tool is usually unable to identify their origin and licence, and will, therefore, either ignore them or flag them for later manual analysis, which can be difficult, time-consuming, and ineffective. Therefore, such resources should be carefully documented if they are used.
- Most software projects developed within GÉANT have LICENSE files in their root folder, which is the default place other developers look at. However, this may not be sufficient, especially if multiple licences are offered. Even if software is kept in a state suitable for a particular intended licence, this

licence is often not indicated in the documentation. The most suitable place for this is a README file. Similar to many other OSS projects on the internet, authors often assume that it is sufficient to provide the standard licence text in the LICENSE file in the project's root folder. The copyright statement and history of changes may also need to be checked and updated if required by the licence.

- While Python itself is released under the permissive Python Software Foundation License, many commonly used Python libraries are released under other open source licences, which can have implications for the licensing of the code that uses those libraries. It is, therefore, important to check these licences as they may affect the licence of the resulting product.
- Java is less problematic regarding the licensing of commonly used libraries, as standard libraries, APIs, and frameworks are contained in Java runtime environments or containers for which permissively licensed implementations are readily available. However, it is important to make sure that an appropriately licensed environment with all the necessary features is used.
- The operating system used, such as Linux or MS Windows, or the container, such as Docker or Kubernetes, is unlikely to affect the licence of the code running on them unless a very custom setup is used, or the code is linked or distributed with the Linux kernel. However, SCA tools may show different dependencies in their reports. Mend used to produce significantly varied reports depending on the platform used but they are now quite consistent.
- Software developed in the GÉANT project should indicate copyright. Some GÉANT projects have their copyright notice in the LICENSE file, which is a standard practice only for the MIT licence. However, the copyright notice should also be included in a separate COPYRIGHT file in the root folder of the project. This file should include the copyright notice of the GÉANT Association and/or listed contributing partners or organisations owning copyright over parts of the work. The notice should reference all previous GÉANT project phases during which the software project was also active, and should state the current year.
- As a matter of best practice, a number of other files should be included in GÉANT software projects: NOTICE, to declare and credit the use of other IP, their licences and licence options; CHANGELOG, to indicate versions, dates, tags of additions, and changes or fixes; CONTRIBUTING, with instructions for contributors; and a CONTRIBUTORS or AUTHORS file listing people who have contributed to the project.

## 3.4 Changing Role of Software Developers

The GÉANT project, drawing on over 20 years of experience, is adapting to evolving compliance requirements by fostering a culture of heightened awareness about the criticality of OSS licence compliance and compatibility. Initially, developers tended to show indifference towards these issues due to a lack of understanding regarding the repercussions of non-compliance. However, greater understanding and awareness are now being cultivated within the GÉANT project, leading to a shift in attitudes. Previously, developers often perceived compliance as potentially limiting their freedom to select libraries that would facilitate the creation of high-value software; now, however, they recognise that compliance is advantageous for both them and their projects.

Following the update of the IPR Policy, ongoing discussions on OSS have been accompanied by awareness-raising initiatives and training sessions (described in Section 3.5). Additionally, information-sharing sessions on software composition analysis scanning and licensing have been conducted, with more events planned by the IPR Coordinator and WP9 Task 2.

Initially, the focus of the licensing team in GN4-3 was to encourage software developers to move past neglecting licences and start considering OSS licences through engagement in SCA. This involved helping them understand the GÉANT IPR Policy drafted in GN4-3 and enforced since the beginning of GN5-1, encouraging them to request SCA, reducing initial obstacles to engagement, and encouraging them to analyse and discuss identified libraries and their licences. An onboarding package for software developers covering best practices, IP and privacy issues, and actionable recommendations at various levels was prepared. However, during OSLS work, it became

apparent that these recommendations should be transformed into more prescriptive instructions. Therefore, for over a year, the OSLS has shifted its approach to developers, encouraging them to take greater responsibility for the application of and compliance with the selected process. This does not mean developers should take full responsibility for the licensing process but that they should lead in the parts for which they are best suited. The parts of the licensing process that should primarily stay with the OSLS team are those related to licence compatibility analysis, licences selection, and use and customisation of the used SCA tool, as they are too cumbersome for most software projects and require a steep learning curve.

In the latest group of software projects seeking both SCA and SLA, there has been a notable shift in support dynamics and needs. These projects are not just focused on obtaining reports and managing dependencies at their own pace but also include a significant preparatory phase with software development teams seeking clear instructions for effective licence compliance, and who also need to define more precisely the scope of the analysis and properly register their projects into GÉANT's software development related services. Therefore, the related background work of the OSLS has been extended to include engaging and educating developers on the need to amend their software and related artefacts and documentation, providing actionable information, and actively educating them on what they should do.

This change entails moving beyond merely analysing and discussing licences to providing clear instructions on specific actions developers can and should take regarding licensing. Developers prefer such instructions over in-depth knowledge of licensing intricacies, focusing on how these can be properly applied. They are interested in clear instructions on declaring software licences in software repositories and other steps that ensure full licence compliance. However, as selecting licences and addressing potential problems requires commitment, software project managers should also be the focus of additional awareness-raising activities and receive a clear message from GÉANT prioritising resolving licensing issues and declaring licences for their software. Only when a significant proportion of software projects have embarked on this path should a campaign to enforce the GÉANT IPR Policy be launched, otherwise it would face a backlash. Without building this urgency, projects will continue to prioritise running associated services and perfecting and optimising software, and implementing features on their roadmaps. This is understandable as, based on GÉANT developers' experience, IPR and licensing issues were not perceived to lead to legal or financial liabilities. Without proper awareness and training, engineers and developers are more likely to focus on issues within their expertise that bring immediate benefits and praise, viewing other topics as suitable for lawyers and an extra burden.

Some software projects have made changes to their dependencies and want to use SCA reports to assess the impact and progress made. A significant proportion of SCA scans are candidates for repetition, providing an opportunity to assess improvements, new dependencies, and outstanding issues. This also allows findings to be clarified and outstanding questions on report details or remedial actions to be addressed.

Only a few projects expressed interest in continuous SCA through CI/CD integration, indicating that licences are not considered daily responsibilities but are reviewed periodically, which is justified as long as newly added dependencies are managed properly.

While automation is of interest among developers, as they hope that it will handle most of the licensing management and spare them manual labour, the expectation of "full" automation is deemed unrealistic given the current capabilities of SCA tools, the non-selectivity and verbosity of the alerts they produce, and the absence of their capability to automatically determine or suggest potential outward licences. However, developers are interested in vulnerabilities and reports about deprecated libraries generated by Mend, offering immediate benefits and driving wider SCA integration into CI/CD toolchains.

In most cases, developers prefer to keep SCA reports private, which is justified if they identify licensing incompatibilities or library vulnerabilities. However, sharing results could encourage others to work on licensing improvements. To address concerns regarding vulnerabilities, incompatibility and potential liabilities, user access controls have been established to regulate access to the Mend service, software projects' dashboards

and SCA reports, considering the sensitive nature of potentially exposed information, including detected vulnerabilities in used libraries [Wiki_MendAccess]. The unified user authentication operates through GÉANT single sign-on (SSO) and eduTEAMS [eduTEAMS].

To simplify its message, the OSLS focuses on Mend features related to licences, presenting its vulnerabilities-related support as an additional benefit from SCA and a part of managing project dependencies. Deeper security matters are left to the WP9 Task 2 Security team [Wiki_SCT].

Improving attitudes towards OSS use involves raising awareness and explaining the benefits of considering licence compliance and compatibility at the outset of software development. The IPR Coordinator continues to work closely with WP9 Task 2 to provide more infoshares and OSS training.

A multi-phase feedback mechanism [Evaluation_Survey] has been established to gather input from end users and administrators. This mechanism is aligned with other feedback loops and is crucial for identifying improvement areas, addressing user concerns and continuously enhancing the effectiveness of the licence management system. The Open Source Review Board (OSRB, described in Section 3.7), through its members from product and service management and software development communities, also serves as another instrument for collecting user ideas and feedback at strategic level and beyond individual project experiences.

## 3.5 Awareness Raising and Training

During GN4-3, the licensing team recognised the need to increase awareness among software development teams regarding the use of OSS and its associated requirements. Initial training, focused on OSS licence compliance and compatibility, took place in February 2022 [OSLC_Training]. The following month, a follow-up webinar on licence dependencies analysis with WhiteSource (now Mend) [LDAwithWS_Webinar] showcased the features of this SCA platform and its role in licensing and library management and how its use is supported by the licensing team.

In GN5-1, these efforts continued to promote and increase implementation of the licensing process for software developed within GÉANT, including already-produced software, and ensure new software projects apply appropriate licences while addressing their dependencies' licences. Efforts to enhance user awareness of licensing, SCA and SLA services provided by OSLS have been ongoing since the start of GN5-1, accompanied by the development of guides (see Section 3.6) and training initiatives focused on the practical application of OSS licences. The organised events and training sessions aim to:

- Increase awareness of and responsibility among software developers for software licence management.
- Enhance understanding of open source licences through real-life scenarios.
- Engage developers through attractive and user-friendly training materials.
- Motivate developers to use available support and tools and to request SCA and SLA services.
- Provide practical information for assessing components and selecting project licences.
- Enable developers to effectively apply recommended or selected licences.
- Raise awareness about the additional benefits of using Mend.

The IPR Coordinator and WP9 Task 2 created an onboarding pack for software developers, including software best practices, IPR, and privacy issues [Pack]. The related infoshare dedicated to best practices, IP and privacy for software developers took place in March 2023.

In April 2023, the second edition of OSS licensing training took place [IntroOSLC_Training], which included additional information and an example from GÉANT.

In October 2023, an infoshare on software licence management in GÉANT provided insights into software project management, licensing and privacy practices within GÉANT [SWLMinGN_Infoshare]. Attendees were informed about scanning codebases for open source components and licences, resolving licence conflicts and obligations, selecting appropriate licences for projects and automating licence management. The session also covered aspects such as producing licence and copyright artefacts, and adhering to the GÉANT IPR Policy and recommendations. In addition, participants were informed about leveraging WP9 Task 2 services for comprehensive software governance and support, including SCA and SLA services and how to use them.

A lightning talk *Establishing a Licence for Your GÉANT Software* was held at the GÉANT Project Symposium in December 2023 [GPS2023_LT]. Again, the OSLS team and IPR Coordinator covered the tools and expertise available to help streamline licence management.

To further involve and empower software developers, a recent March 2024 infoshare *OSS licensing and licence compliance guidelines for software developers* [InfoShareGuides] promoted two guides – *Software licence selection and management in GÉANT* [SLS&MG] and *Important licences for licence selection* [Wiki_ImportantLicences]. This infoshare concentrated on licence selection and management, and related software project artefacts such as README files, LICENSE files and CHANGELOGS, and discussed the compatibility of commonly used OSS licences. The practical use of these documents was emphasised by giving an overview of efficient preparation, information gathering, and proper software licensing by walking through the first guide. The aim was to furnish participants with insights into how this guide supports compliance with a selected licence, through detailed implementation instructions and in-depth information on creating essential licensing artefacts. Additionally, the infoshare emphasised vulnerabilities related to third-party libraries and reiterated the support provided through SCA and SLA services.

All these infoshares and training sessions were recorded and are now part of GÉANT's eAcademy.

Another infoshare is planned for Q3 2024, aiming to enhance understanding of vulnerabilities and licensing issues associated with third-party libraries. This collateral topic seeks to further highlight the importance and usefulness of the support provided by WP9 Task 2 and the IPR Coordinator in the realm of open source. Participants will also gain insights into Mend's ability to identify vulnerabilities and ensuring licence compliance.

The events described above are part of GÉANT's broader effort to raise awareness about OSS, licence compliance and compatibility and to empower software developers to deal with them. For all of these events, participants are expected to have a very basic understanding of open source software, and the events and materials are designed to be useful for participants with different backgrounds. Familiarity with a typical software project structure and source code repositories is welcome but not required. These events and materials remain useful for leaders responsible for developments within the GÉANT project, task and activity managers, team leaders, software developers, and engineers actively contributing to open source projects or developing internal projects using open source code. This approach shift aims to broaden awareness of and engagement in software licensing.

The coordination and logistical support for event arrangement, preparation, promotion and presentation rehearsal have been provided by the GÉANT Learning and Development (GLAD) team. The IPR Coordinator and WP9 Task 2 plan to ask GLAD for further support in creating more effective learning materials. For example, the recently produced guide for developers *Software licence selection and management in GÉANT* [SLS&MG] could be complemented with a transcript from the related infoshare, incorporating details from other, previously developed materials on open source licences and supporting tools. The IPR Coordinator and WP9 Task 2 will also ask the GLAD team for support to prepare the information in a more condensed and interactive format or transform it into a self-paced online GÉANT eAcademy course, containing compelling infographics on topics such as OSS, IP management, security significance, and licensing and compliance within the GÉANT project. Another potential area for elaboration for the OSLS team is the use or creation of data (including personal data) with OSS, although this is not directly within the scope of the OSLS team. Cross-promotion between various WP9 Task 2 teams and synergy in adopting their support and review services could also be beneficial.

There are emerging plans to apply digital badges to support software licences, which were discussed as a possible use case for software governance quality badges at the 2023 Project Symposium [GPS2023_SB]. Potential development of OSS and licensing-related tests for individuals could be introduced in the future.

## 3.6 Documentation and Guides

Since GN4-3, the licensing team has been diligently collecting and consolidating information about OSS licences, and elaborating on their differences, compatibility, and usage. They have also been writing internal guides, procedures, and documentation for using Mend, as well as maintaining and enhancing the existing guides and wiki pages. For instance, a detailed yet relatively generic guide on open software and licensing, along with related topics such as *OSS licences and licence selection* [Wiki_OSSL&LS] and a reference wiki [Wiki_OSSL_RefInfo] were initially published towards the end of GN4-3. The latter provides extracts of key information and pointers to resources on OSS licences, compatibility matrices, useful tools and related articles and resources. Parts of this information were also highlighted in a later developer-oriented guide [SLS&MG]. This material was updated during 2023 and served as a foundation for subsequent guides such as [Wiki_ImportantLicences] and [Wiki_OSSLWP].

At the beginning of GN5-1, the OSLS team summarised their experiences in a GÉANT-oriented white paper on software licence management, which was published in March 2023 and distributed to GÉANT software teams [Wiki_OSSLWP]. In addition to maintaining and updating previously developed materials, the OSLS team has shifted its focus to producing guides that cover actions developers can and should take regarding licensing. This shift was in response to the evolving needs of software developers, who have begun transitioning from SCA-based checks to licence selection and implementation with SLA.

To support this approach, additional documentation has been prepared to guide developers through SLA/SCA scans and associated actions. These topics include elements of software licence selection and management for developers, as well as the creation and maintenance of related project artefacts.

For example, the *Software licence selection and management in GÉANT* [SLS&MG] guide delves into the complexities of licence selection, declaration, compliance and associated tasks, offering a step-by-step elaboration for software development teams. It provides practical hints and examples tailored for software developers. The first part outlines key aspects of software licensing for developers, emphasising tasks, collaborative processes and essential elements for efficient preparation, information gathering, and compliance. The second part offers detailed guidance on implementing the chosen licence, providing instructions and critical insights to facilitate the creation of necessary artefacts (LICENSE, README and COPYRIGHT files) and optional ones (such as NOTICE, AUTHORS, CHANGELOG and CONTRIBUTING files). It is intended that this guide will serve as a foundation for GLAD eAcademy training materials.

The *Important licences for licence selection* [Wiki_ImportantLicences] document highlights essential OSS licences and their requirements, providing a concise overview of licence categories and presenting licences from each category in alphabetical order. It summarises the licences commonly encountered in GÉANT software projects as detected by Mend, as well as a few that could pose problems or are otherwise relevant for GÉANT software projects. The document aims to facilitate compatibility analysis and licence selection to assist software developers in understanding their responsibilities related to these licences. It also includes a major update of an earlier published diagram of licences in GÉANT. The work on licence descriptions and the diagram summarising their relations was done in parallel, supporting the conceptual refinement of each; therefore, the diagram expresses the essence of relationships between the discussed licences in a condensed form. This document is based on the internally developed database of all detected OSS and other licences, and overview tables from the OSS white paper. It is not intended for end-to-end reading or detailed learning but to assist in interpreting licence requirements, compatibility and understanding the ramifications of selecting a specific licence.

These documents will undergo testing and adjustments over the coming months. The OSLS team will also continue to update and consolidate the developed guides and provide information about other significant concerns, topics and additional licences in GÉANT software projects as they become relevant.

## 3.7 Open Source Review Board (OSRB)

A key part of the OSS governance framework in the GÉANT project is the Open Source Review Board (OSRB), which collaborates with the IPR Coordinator to oversee open source management, providing practical guidance, feedback and direction for operational-level OSLS decisions. It integrates perspectives from software development, IP governance, and product, project and service management by engaging practitioners from each of these areas.

The OSRB interfaces with stakeholders, contributes to GÉANT's strategic approach to IPR, proposes refinements to the GÉANT IPR Policy and to knowledge-sharing and licence selection processes, and provides input to awareness-raising and training. Its decisions are based on, and may also influence, established licence management policies, practices and procedures. It can also prepare and submit questions or proposals for the GÉANT Oversight Committee and its appointed IPR Committee focused on the application and enforcement of the GÉANT IPR Policy and provide input on licensing and IPR decisions to protect project IP.

The OSRB's role and composition was defined in May 2023 and its members recruited in June. The highlights from its first meeting in July were to streamline the licensing process and apply automation where possible, along with raising awareness. In February 2024, the direction towards empowering developers to comply with licences was affirmed, and the members agreed to engage in testing and refining of guidance, training and awareness-raising materials. Its meetings take place every few months or as needed for significant issues. The next meeting is planned for April 2024. Further information about the OSRB is provided on the GN5-1 Software Governance wiki [OSRB].

# 4 Licence Management Workflow

A comprehensive description of licence management in GÉANT, encompassing preparation, information gathering, documentation, remediation, creation of licence-related artefacts, compliance and continuous management, is provided in *Software licence selection and management in GÉANT* [SLS&MG]. The central four steps (information gathering, documentation, remediation and creation of licence-related artefacts) are also covered by [OSLC_Training] and [IntroOSLC_Training]. This process is often iterative and repetitive, triggered by the addition of a new dependency, a licence change, a major software release, or taking place at regular intervals. Similarly, the WP9 Task 2 best practice on managing sideground IPR [GN_BP_B6] describes the overall process of software composition and licence analysis, and licence selection, as three interrelated and interwoven flows that support each other [SideIPR].

This section presents an overview of licence management workflow steps, expands on the role of the software composition analysis and software licence analysis services within the workflow, and considers the practicalities of complying with a selected licence. It also discusses automated analysis and reporting, a topic which is frequently mentioned but about which there are often misperceptions.

## 4.1 Overview of Workflow Steps

The GÉANT project OSS licence management workflow is shown in Figure 4.1 and described below.

**Preparation** for a software project involves basic steps such as deciding on the software name, subproject grouping, and use of external contributions. Internal considerations include addressing authorship and deciding on copyright, which typically defaults to GÉANT. For new projects, building a proof of concept solution is advisable to understand the necessary components and their licences. Existing projects should gather and consolidate their information and documentation. All software elements must be consolidated in GÉANT GitLab [GN_GitLab] or GitHub [GitHub] and registered in the GÉANT Software Catalogue [GN_SC]. Non-original artefacts and assets, especially those that are not software components, should be documented with their origin, copyright and licence upon addition to the project to avoid identification issues later.

The creation of plugins or inclusion of modules or plugins for existing software and platforms may be problematic. Thus, a decision on the scope of licence management scans should be made, focusing either solely on the plugin or including the wider platform. Decisions should consider platform conventions, community conventions, customer expectations and plans for the future.

When managing interconnected projects or products, it is preferable to keep components in one GÉANT GitLab project, while GitHub can be used for public visibility or to expose just the project's "community" part. Maintaining a holistic view is crucial to avoid issues with reusing, repackaging or rebranding elements. Consultation with licensing and the GÉANT Marcomms Team (marcomms@geant.org) is recommended.

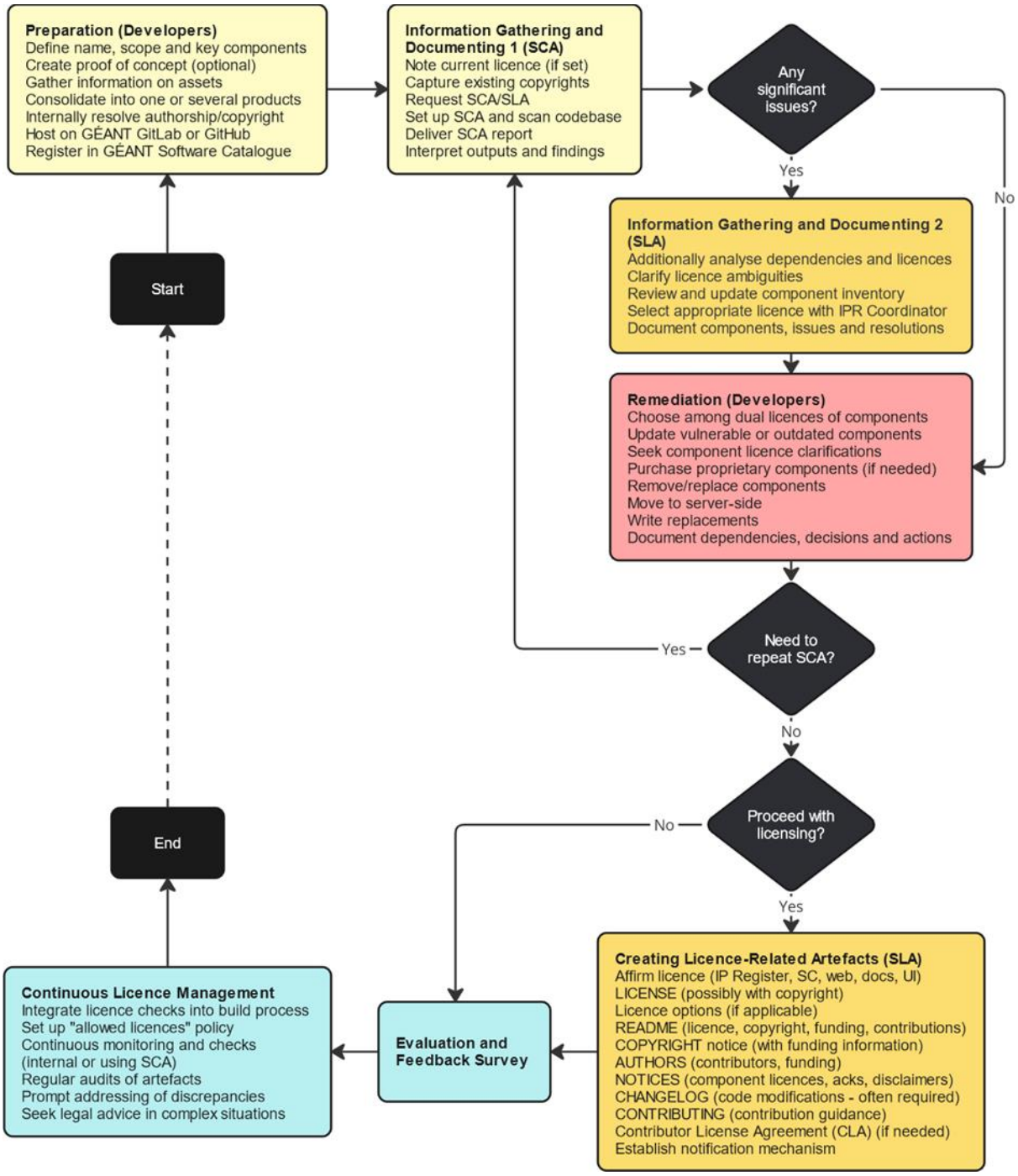


Figure 4.1: GÉANT project OSS licence management workflow overview

**Information gathering and documentation** involve capturing existing copyrights, licences and decisions. To achieve this, the use of the GÉANT SCA service followed by the SLA service is recommended; they are requested via tickets in GÉANT Jira [Jira RSWR]. After scanning the project code with the SCA tool, the inventory is to be reviewed and updated based on findings. Some SCA results will need correction, after which components to be modified (vulnerable, outdated, or inadequately licensed ones) are identified. The licensing team and IPR Coordinator assist in making these decisions. All components, licences, clarifications, and remediation decisions should be documented.

If the SCA identifies no significant issues and the current or proposed licence is clear and agreed upon with the IPR Coordinator, additional analysis can be shortened or skipped. Also, if developers initially request SCA only, without a subsequent SLA, it is assumed that they prefer to make their own remedial corrections to their project based on the SCA results, working at their own pace, before deciding in due course that they are ready for SLA and the final selection and implementation of a licence. The changes made during remediation, or a significantly postponed SLA, may require a repeated SCA to clarify the situation, validate corrections made, and facilitate the resolution of remaining issues.

**Remediation** aligns the software with the selected licence by resolving licensing conflicts and updating vulnerable components. Developers are advised to start with easy-to-achieve improvements, address key components, repeat SCA if necessary, and document the new state. Dealing with incompatible licences and vulnerable libraries may be complicated, involving removing unnecessary components, replacing them with existing equivalents or newly created replacements, or changing the system architecture (e.g., by moving some functionality to a central service).

**Creation of licence-related artefacts** serves to declare the licence in the source code and repositories. It includes providing a LICENSE file, declaring the licence in the documentation, repository and application UI, and in the GÉANT Catalogue, adding a copyright notice in a COPYRIGHT file, declaring the use of licence options (such as application of later licence versions), publicly documenting code modifications and dependencies (if required), preparing a Contributor License Agreement if external contributors are anticipated, and optionally establishing a licence notification mechanism to alert about changes of licensing terms. The requirements for individual licences are described in *Important licences for licence selection* [Wiki_ImportantLicences].

The licence implemented during the creation of licence-related artefacts must still be approved by the IPR Coordinator. This step in the licence management workflow, which includes scrutiny by the licensing team of the necessary licence- and copyright-related files of the software project, requires developers to update these files in accordance with instructions provided.

At the end of the licensing process, software developers provide feedback by completing a survey covering all performed steps [WP9T2_ReviewFB].

**Continuous licence management** tracks and maintains licence compliance by integrating licence checks into the build process (by using the Mend service provided by GÉANT or other available tools [Wiki_OtherSCATools]), establishes continuous monitoring of components, licences and compliance, conducts regular audits of licence-related artefacts, and seeks legal advice from the IPR Coordinator when necessary. Some tools such as License Maven Plugin [LMP] can download dependencies' licence files, check, update or remove licence headers in source files and update (or create) the main project licence file.

Continuous licence management is carried out by the software development team based on the SCA/SLA experience and advice from the licensing team, who may also participate in this integration by adjusting the project configuration in Mend and configuring it for the chosen allowed or prohibited licences. Although further monitoring and adjustments may be performed by the development team after a successful licensing, it is recommended that after a significant passage of time, or significant new licensing issues, or major changes in software, the entire SCA/SLA sequence be repeated to ensure the project remains in good shape.

## 4.2 Software Composition Analysis (SCA) Service

This service assists software development teams by establishing a project within an SCA tool and providing valuable insights into external components. It is suitable for **one-time software analysis** but also **continuous monitoring**, identifying third-party components used and their licences, and offering information about potential IPR infringements and security vulnerabilities. The service can be used in combination with other software review services or performed exclusively. Repeated analyses can determine how changes in software

and dependencies impact licence compliance and identify new or pending vulnerabilities. For ongoing monitoring, the produced analysis setup can be integrated into the project's continuous integration platform.

The SCA is currently based on Mend (described in more detail in Appendix A), which is used to identify third-party components in projects and gather information about their licences and security vulnerabilities. Mend employs a comprehensive database to assist in two critical aspects:

- The analysis of components and their licences helps reduce risks associated with IPR infringements, which could have significant financial consequences, by achieving licence compatibility and compliance.
- The security of OSS is another important issue. Mend reports vulnerabilities through a report that complements SonarQube and extended code reviews.

The licensing team sets up the project in the Mend SCA tool, which generates reports on the software composition and potential deviations from established policies.

The visibility of produced reports and the created Mend project can be established while the software project is being set up, but can also be adjusted after the results of the analysis have been obtained or even at the end of the review.

The primary report ("Risk Report") is on the software composition with its components, their licences and related risks and vulnerabilities.

The designated leader or expert from the software development team receives this report and provides support in interpreting it, although the software development team should be able to interpret this report themselves.

The licensing team helps with this report if needed, and the developers can ask for additional feedback on the reported and other risks related to licences and IPR infringements.

A summary of the SCA service is available in *Software Reviews* [Wiki_SWReviews], with additional details in the *Client Guide for Software Composition Analysis (SCA)* [Wiki_CGSCA].

## 4.3 Software Licence Analysis (SLA) Service

The SLA service is a technical consultancy service designed to provide a comprehensive understanding of third-party libraries within a software project and their licences. This understanding is crucial for selecting appropriate software components and the software licence applied and for ensuring compatibility among all licences involved. The service is recommended for software development teams seeking to validate third-party licences, establish or review their software's licence, ensure compliance with it and the GÉANT IPR Policy, or assess the implications of potential changes in the project licence or changes in licences of used libraries or frameworks.

To utilise the SLA service a prior software composition analysis is required. The service then builds upon the SCA results, complemented by manual checks of detected libraries as necessary. It involves customising the licence settings of the SCA tool, project licence selection with an analysis of the relationship between the project licence and those of its dependencies, and checking alignment with licence requirements and the GÉANT IPR Policy. This process also verifies related documentation artefacts. If the SCA tool is used with continuous integration, the service team collaborates with the customer to tailor related settings.

The decision as to which project licence to select depends on project goals, developer preferences, collaboration needs and constraints imposed by dependencies and other intellectual property. In some cases, the most restrictive licence compatible with all those present may be necessary. However, this is not always the case, especially when permissive licences have been used. Furthermore, at times, a licence that is compatible with the most, or with all, may not even be among those that are present. The selection process also considers the

effort required to remediate licence compatibility and libraries' security problems, assess the impact on the software's ecosystem, and ensure compliance with legal and funding requirements. The chosen licence not only fosters a collaborative and transparent development environment but also provides clarity on usage and contributions to the open source project. All of the above illustrates the complexity of licence selection, and explains why the SLA service was designed and is needed.

For more detailed information on the SLA service, refer to *Software Reviews* [Wiki_SWReviews].

It is important to note that the use or modification of externally developed work, particularly database models and architectural designs, can impact software licensing. This includes embedding external data necessary for software operation, and also applies to data in external code libraries or modules. Typically, the same open source licence applied to software extends to original assets kept in its source code repository and distributed with it, such as embedded data, technical documentation, configurations and user manuals.

Independently distributed artefacts and assets may have different licences. Creative Commons Attribution (CC BY) and Attribution-NonCommercial (CC BY-NC) are suitable for tutorials, presentations, standalone training and promotional materials.

Acknowledging external data in documentation is vital for transparency and adherence to licensing terms. While dynamically retrieved data may pose fewer problems, it should also be documented prominently. The processing of user-created or external data should be described clearly, explaining its integration and compliance with legal requirements.

## 4.4 Complying with a Selected Licence

The second half of *Software licence selection and management in GÉANT* [SLS&MG] provides developers with instructions on what they need to do after selecting a licence. The instructions facilitate preparatory work and internal compliance checks before reviewing licence adherence with the licensing team. They also provide essential information for developers seeking to address licensing issues independently.

**Developers are obligated to adhere to the requirements of the chosen OSS licence** and ensure licence compatibility. Failure to comply constitutes a breach, potentially leading to legal challenges and significant financial loss.

Even if the software and its dependencies are aligned with the chosen licence, this **licence must be clearly stated** in the documentation, including the README file. Most licences require a copy of the licence to be included, typically in the LICENSE file in the root folder. Some licences may only require their name or URL in documentation, but having the licence text in a dedicated file is standard. A clear and explicit statement of the specific licensing is necessary, beyond just including the licence text. For instance, the GPL family of licences articulates this requirement in the "How to Apply These Terms to Your New Programs" section at the end of their text. Simply including the licence text in the LICENSE file is insufficient; a distinct statement affirming the applied licence is required.

While licence and copyright information usually do not need to be in every source file header, the applied licence and funding should be clearly declared and strategically placed so that anyone interested could easily find and see them. If the software has a website or webpage, the licences should also be stated there. The source code repository used may have a mechanism for specifying the used licence. GitHub and GitLab provide features that allow declaration of the licence by using the repository's user interface. GitHub can automatically recognise the used licence from the LICENSE file in the root folder, but not the licence options applied to the project.

Software authors may specify alternative licences for a project, offering it under a dual licence or multiple licences. However, when such software is used in another project, only one of its available licences is applied

when considering compatibility with the licence of the main project. Also, the component's licence must be compatible with the licence (or all offered licences) of the main project.

The minimal set of typical documenting files in a software project usually includes README for project information, LICENSE for licensing details and CONTRIBUTING for contribution guidelines. The applied licence may require the inclusion of CHANGELOG or CHANGES for tracking project changes. These files may optionally use markdown when their names end with the .md extension. If so, they can be edited using an online markdown editor or checker such as Dillinger [Dillinger] or StackEdit [StackEdit].

[SLS&MG] discusses the following compliance requirements in more detail, often with markdown templates, explaining the placement of various licence, copyright and software-related information. Additional templates and links to example files with GÉANT-approved content will be provided as they become available from software projects.

- A README file is the starting point of software documentation, providing key information and guidance. It should succinctly describe the software's purpose, scope, installation and usage. It must cover the software's licence, copyright, acknowledgements and, potentially, roadmap and community contributions. A recommended template is available at Make a README [Make a README], offering a sample markdown file and detailed suggestions for creating an effective README.
- Providing just a LICENSE file with the licence text is common practice but is not sufficient. The applied licence may offer additional options defined within it, including optional licence possibilities, conditions and permissions that must be activated by additional statements. Some common examples include: permitting users to choose between the original licence version or any later version, relicensing under a different licence, extending certain rights beyond standard terms, placing limitations on certain uses or modifications, and choosing the jurisdiction under which the licence is governed.
- Complying with licences of used code requires addressing the obligations imposed by licences governing dependencies or reused code, and adhering to associated copyright and patent rules. This is done by extending README, COPYRIGHT and NOTICE files to declare and credit the use of other IP, their licences and licence options, or by retaining all preexisting licence- and copyright-related files and notices, attributing and documenting modifications to reused code and staying up-to-date with changes of used code and its licence.
- A COPYRIGHT file indicates copyright for software developed in the GÉANT project. Copyright statements are crucial in addition to declaring a licence. There is recommended copyright and disclaimer wording for GÉANT projects, which should also cover all iterations of GÉANT during which software was developed. It should include other statements confirmed by the IPR Coordinator addressing contributions by other partners. It should also satisfy the EU funding requirement to include the EU emblem with specific formatting.
- A simple copyright line and a licence indicator placed in the header of source files are useful if individual project files may be accessed, reused or modified independently.
- Places to acknowledge contributors, dependencies and used tools are AUTHORS, NOTICE and README files. An AUTHORS file lists project contributors, their roles and optional contact information. It can also mention funding sources. Dependencies from directly used third-party libraries, tools or other projects may be acknowledged in a separate NOTICE file or README section, with details such as version number, URL, licence and copyright holder. Acknowledging contributions and dependencies shows appreciation and fosters collaboration within the open source community. This documentation should be regularly updated as the project progresses.
- A CHANGELOG file tracks changes made to a software project over time. It helps users understand what's new in each release and how the project is evolving. In the CHANGELOG, the newest changes appear first, with version numbers, tags, or dates. Individual changes are summarised in bullet points or brief paragraphs describing the changes and their types, along with brief explanations of why they

were made and optional links to commits or issues. The provided information could be based on commit messages, release notes and other project records.

## 4.5 Automated Analysis and Reporting

Automated Mend reporting generating regular reports on licence usage was implemented in one project using Bitbucket, a Git-based CI/CD tool. The OSLS team plans to replicate this with GitLab for another project team that has expressed interest. These reports facilitate proactive decision-making and ensure compliance with selected licences. Despite being an appealing alternative to periodic SCA service use, it has limited utility. Mend is currently unaware of changing project versions, resulting in the loss of project data with each new source code scan. Additionally, the tool cannot produce differential reports, leading to redundant information in consecutive reports, without the ability to alert about new dependencies or licences.

Upon discovering these limitations, developers' interest in SCA automation by integrating Mend into their build workflows typically decreases. Also, implementing it would require them to engage in customising their build toolchain and assume responsibility for interpreting the reports. Consequently, this greatly diminishes the interest in SCA integration with GitLab. Instead, software teams find it more convenient to occasionally request the SCA service, letting the licensing team identify and point out significant changes. With SCA, different versions can be scanned as separate Mend projects, preserving their history.

The announcements and previews of other products made by the producer of Mend suggest a shift towards recognising software versions, potentially resulting in improved differential reports and alerts on software components and licences. However, for reasons unknown to the OSLS team and about which it can only speculate, this has not yet been realised.

Furthermore, existing tools, including those by other companies, do not effectively support or automate SLA due to noise in SCA-produced data on libraries and licences and the non-fully-deterministic nature of selecting a subsuming licence based on existing licences, as this process must also assume some residual risks. Therefore, an automated tool could only suggest one or several potential subsuming licences indicatively.

# 5 Recommendations

The following recommendations with regard to open source software licensing in the GÉANT project have been formulated based on established WP9 Task 2 and OSLS team practices and experiences, the GÉANT IPR Policy [GN_IPRPolicy], software licensing support provided in GN5-1, expectations regarding IP management (also see GÉANT Resources – Intellectual Property [GN_Resources_IP]), general OSS-related conventions and practices, and emerging standards in the broader R&E (including Open Science) community. They cover preparation and support; software development; software composition analysis; software licence analysis and licence selection; licence declaration and compliance; copyright management; and overall governance.

**Preparation and support**

- **Awareness** about IPR management, GÉANT IPR Policy and copyright should be continuously elevated among software development managers, team leaders, and team members. Even developers have an opportunity to contribute to licence management by asking about the OSS licence of the software they are working on or whether they can include specific dependencies in it. The same applies to contractors, who should know upfront how to approach libraries, their licences and copyright over the work they are hired for.
- Key people in software development teams should **read the GÉANT guidelines** and tutorials on IPR and software licensing, and **attend the related training sessions** until they are sufficiently familiar with the subject. The people working on IPR and software licensing in GÉANT try to make it as simple as possible, but the subject is vast, complicated, and requires a lot of effort and time to master.
- **Start the licensing process early**, and select software licences early on in the development process, as soon as all key requirements and external components are known. This makes it easier to set up a licence and maintain compliance.
- Prior to engaging in licensing, **determine how the project is packaged** into products and software repositories, **and register it in the GÉANT Software Catalogue**.
- If software development teams have any further questions or are in doubt about which OSS licence is best for their project, they should **contact the IPR Coordinator or the OSLS team** [IPRSupport], [Contact].

**Software development**

- **Use software composition and licence analysis (SCA and SLA) services** that conduct related reviews and audits designed to help determine the OSS licence appropriate for the software and ensure licence compliance. Identifying and addressing vulnerabilities in the software that may be detected by the SCA improves its quality and benefits the broader community to which software development teams contribute.
- **Assess the used components and software** by applying common software quality and trustworthiness checklists, to ensure the components used and software produced are reliable. Examples: TinyMCE – Open source software evaluation checklist [TinyMCE_OSSEC], Red Hat – Checklist for measuring the health of an open source project [RedHat_COSP], EURISE Network Technical Reference – Software quality checklist [EURISE_SQC].
- **Graphical or UI resources** such as images, vector graphics, JavaScript code or preset GUI layouts that come from external sources **should be annotated for provenance and licence** within the software repository, the project's Software Bill of Materials (SBOM) or via easily extractable embedded metadata

and comments. Even if they originate from a clearly stated dependency, they may be relocated as required by the used framework, potentially leading to a loss of their origin context. Such resources should be carefully documented when deciding to use them. If this is not done at the time they are included in the project, it can be challenging to trace them back to their source later on.

- It is preferable to place the OSS source code in a public and **versioned code repository** with a clear **indication of the used licence**. GÉANT GitLab is a preferred place for this [GN GitLab].

**Software composition analysis**

- **Every GÉANT project software project should be analysed using the GÉANT-recommended software composition analysis tool and the related service** to ensure licence compliance and compatibility.
- Some **components or their licences may not be correctly recognised** by the SCA tool. This requires a **manual check**, which can be labour-intensive. Fortunately, SCA tools typically support overriding the information about components' licences. Additional dependencies may be tracked in SBOM or, for major components, in either the README or NOTICE file. Manual editing of reports created by the SCA tool is not recommended, as they may easily be overwritten the next time they are generated.
- It is unlikely that the operating system or container used will affect the licence of the code running on it, unless a very specific setup is used or the code is linked or distributed with, e.g., the Linux kernel, or if a proprietary or copyleft component had to be added to adapt software to the specific platform. Depending on the runtime environment, **SCA tools may detect and report different dependencies**. Such cases may need to be manually reviewed. However, if software is designed to run on multiple platforms and the scan for one platform does not indicate any licence risks, incompatibilities or security vulnerabilities, **scans for the other platforms are most likely unnecessary**.

**Software licence analysis and licence selection**

- The **chosen licence must be compatible** with licences of all software dependencies and used components so that the IPR and licensing risks are eliminated.
- Every GÉANT software project should select and **apply a suitable OSS licence** that fits the needs of the software development team and those of the user community. The lack of a clear licence indicates that developers often consider licensing unimportant, confusing, or too time-consuming. Projects where licensing is not addressed properly tend not to last long or build a large community. Use tools that help with choosing an OSS licence.
- Permissive (non-copyleft) open source licences, such as MIT, BSD-based, or Apache License 2.0, are strongly recommended for GÉANT software projects. They guarantee the freedom to use, modify, and redistribute the code. Therefore, **whenever possible, software should be released under permissive licences**.
- **Use strong copyleft licences sparingly and only if approved** by the GÉANT IPR Coordinator. Because software under strong copyleft cannot be incorporated into software under permissive licences, it is advisable to avoid strong copyleft licences. However, their use can be approved if it does not hinder the adoption or reuse of software in the target community and it is mandated by a wider collaboration or necessary for licence compatibility with a critical component. On the other hand, using a strong copyleft licence protects the software from scenarios where the project is relicensed and privatised by a later major contributor. Arguably, however, such scenarios are unlikely in the GÉANT project context.
- **Identify licence conflicts and resolve them appropriately**. The licences of some components may not be mutually reconcilable within a project intending to mix them, as it is not possible to select a licence that would subsume both. The most frequent and often neglected problem of that kind is between GPL 2.0-only and GPL 3.0 or Apache 2.0 and GPL 2.0-only licensed components. Identification and resolution of licence conflicts may involve trivial or easy-to-achieve actions. Sometimes, the problematic code can be relicensed or multi-licensed upon obtaining permission from copyright holders. Complex

interventions include removing or replacing dependencies, developing substitutes, making architectural changes by moving some features to a central service, and refactoring the existing code that relies on those dependencies, substitutes or changes.

- **Be aware of and prepared for situations that require additional adaptation and effort**. Projects that rely heavily on Apache-licensed components may prefer to apply Apache licensing to them. However, if they have any dependencies under GPL 3.0 or AGPL 3.0, they must apply one of those licences (or only AGPL, if it is already present) or opt to eliminate these dependencies. Components with a Mozilla 2.0 licence can be integrated into projects under GPL 3.0 and AGPL 3.0, ensuring that the original files remain available under Mozilla 2.0 terms. Similarly, projects under Apache 2.0 or GPL 3.0 can incorporate libraries under Eclipse 2.0, provided they clearly indicate the use of these libraries and their licence, and include the Eclipse licence text and the libraries' source code. Furthermore, if the combined code is distributed under GPL 3.0, it must be stated as Eclipse's Secondary License for code licensed under Eclipse 2.0.
- The licence to be used for **a product that is part of a broader portfolio should be considered together with other related products**. Using one or a few compatible licences simplifies the situation for users and makes it easier to recombine, repackage or share the code.
- Software-related **artefacts** (technical documentation, configuration, and user guides) **distributed with software or kept in its source code repository should be under the same licence as software**. For **separate tutorials, presentations or standalone training or promotional materials**, the **CC BY-NC or CC BY** licence is recommended.

**Licence declaration and compliance**

- Software development teams must **comply with the requirements of the OSS licence** they have chosen and ensure that there is licence compatibility. If they have not complied with the licence requirements, they will be in breach of the licensing conditions, which may result in significant financial loss.
- **The licence applied must be clearly stated** in the documentation and by copying the licence text into the LICENSE file in the project's root folder or another file as required by the licence. Among other things, the README should clearly state the software's name and explicitly tie it to its intended purpose, scope of application and the applied OSS licence; in other words, the identifying and meaningfully bounded name should be linked to the licence in a clear way in and in a single document. The source code repository used may also have a location where the licence used should be specified (usually in the project settings). If software has its own website or webpage, the licences should also be stated there.
- **Modules located in subfolders may have their own licences**. They should include a separate LICENSE file in each subfolder that contains modules with a different licence than the main project, and provide any necessary attribution or copyright notices for that module.
- Software and its licence, as well as the associated background IP and sideground IP, should be recorded in the **GÉANT IP Register**.
- The **copyright statement and history of changes** should also be reviewed and kept up to date if required by the licence.

**Copyright management**

- Software is protected by copyright law. The variety of OSS licences with different requirements allows software developers to grant other users the rights specified in the licence while preserving copyrights. It is therefore crucial that developers appropriately **indicate the copyright in addition to a licence**.
- **Copyright information must indicate GÉANT's involvement and support**. This information underscores that work was conducted within the GÉANT project or received support from it and identifies who authored the produced software. A COPYRIGHT file in the root folder of the project should include a reference to the GÉANT project and the years in which the work was carried out.

- If the work contains contributions from NRENs that originated independently of GÉANT, or direct insertions or adaptations of code from other projects, their copyright should also be included or preserved if they were already present.
- For some licences, such as **MIT**, the **copyright is an integral part of the LICENSE file**.

**Overall governance**

- **Set up contribution, communication and governance workflows** that ensure compliance with the software's licence.
- Individual participants and stakeholders in the licence management process should undertake **appropriate responsibilities within their areas of expertise and comfort**. The process should be designed to respect this.
- If applicable, **enable and advise on the citation and referencing** of software in scientific papers, presentations, tutorials, etc., ensuring that these references are unambiguous and permanent.
- **Adhere to the standards of the domain community** in software development, licensing, provision of metadata about software, documentation, registration in relevant community registries, citation and promotion of software.

# 6 Conclusions

In response to needs first identified in 2019, and building on the significant IPR and software licence management efforts initiated in GN4-3, the Open Source and Licence Support team in WP9 Task 2 provides comprehensive OSS and licensing support to GÉANT's software developers with the objective of ensuring compliance with GÉANT's IPR Policy, maximising the benefits of OSS and minimising the risks. As described in this report, the OSLS team, working closely with the IPR Coordinator, provides technical and implementation support for OSS management and strategy, including software composition and licence analysis services and tools; awareness raising and training; documentation and guides; workflow; and intelligence and recommendations on implemented licences, typical licensing situations and licensing selection in GÉANT.

The team will continue to deliver and improve these support activities in Year 2 of GN5-1, with next steps and future plans for open source and licence support in GN5-1 and beyond that include:

- Hold further infoshares, including the event currently planned for Q3 2024 on vulnerabilities and licensing issues associated with third-party libraries.
- With the GÉANT Learning and Development (GLAD) team, explore how GLAD might assist with creating enhanced learning materials.
- Investigate opportunities for cross-promotion with other WP9 Task 2 teams and synergy in adopting their support and review services.
- Continue to update and consolidate the existing GÉANT OSS licensing guides and develop new ones to address significant concerns, topics and additional licences in GÉANT software projects as they become relevant.
- Disseminate GÉANT OSS licensing guides more widely, e.g. through Zenodo, conferences, journals.
- Continue to maintain and develop the Software Support Knowledge Base.
- Continue to discuss and develop plans to apply digital badges to support software licences, which were discussed as a possible use case for software governance quality badges at the 2023 Project Symposium [GPS2023_SB], including devising and running a pilot. OSS and licensing-related tests for individuals could potentially be developed and introduced in the future.
- Review the work and purpose of the Open Source Review Board, so as to determine its future role in GN5-2.
- With the Product Lifecycle Management team, explore the idea of enforcing software licences at the production PLM gate and including their consideration at the gate for starting development. However, this measure is likely to be introduced only after most project licences are implemented on a voluntary basis.
- Investigate whether, further down the line, standardised software metadata could be introduced in project files, with a mechanism for their harvesting possibly managed by the GÉANT Software Catalogue.
- Towards the end of the GN5-1, explore options for future work on enforcement and compliance with established product licences and the GÉANT IPR Policy [GN_IPRPolicy].
- Conduct an assessment of the OSLS service elements and workflow, taking into account the continuous refinements based on experience and customer feedback throughout GN5-1. This assessment will focus on understanding the effectiveness of SCA and SLA, particularly in relation to licensing goals, and identifying areas for further improvement.

The biggest challenge for the team is to continue building awareness around OSS licence compliance, hence further cooperation with the IPR Coordinator and GLAD will be continued and further infoshares will be planned.

# Appendix A Licence Management Tools

Software licence management tools, typically referred to as software composition analysis (SCA) tools, aim to streamline and automate processes associated with managing software licences to ensure compliance, mitigate risks, and promote responsible and efficient use of open source software (OSS). They address unique licensing requirements and challenges presented by open source licences. They typically include features such as identifying and cataloguing open source components and their licences, dependency analysis, licence risk assessment, vulnerability detection, documentation, reporting and analytics, review and audit support, and potential integration with software development tools and workflows. These tools can also perform basic monitoring and compliance enforcement, but only for previously specified project licences and within specific licence-imposed and organisational rules, lacking support for open-ended and flexible IPR policies. Additionally, their support for licence selection based on dependencies' licences and project preferences is very limited.

The use of an SCA tool is very helpful for licence analysis and ensuring licence compliance and compatibility, reducing the risk of IP infringements which could have significant financial consequences. The tool used by GÉANT (Mend) also provides additional vulnerability scanning. This is very useful as the security of OSS is another important issue.

Tools for managing commercial licences often provide functionalities irrelevant to OSS and the GÉANT context, such as tracking of owned licences, monitoring of used or misused commercial licences, optimisation of their use, renewal management, and integration with asset management and procurement tools.

## A.1 Mend SCA Tool

The software composition analysis tool Mend (formerly known as WhiteSource) is a cloud-based platform that assists in identifying and tracking the use of open source components in software projects. It was introduced in GÉANT in 2020, and is provided through a service purchased by GÉANT for open source licence and security compliance [Mend SCA]. Designed for in-house use by the customer, Mend does not offer direct legal consultancy. It **detects software components**, **identifies their open source licences** and **uncovers vulnerabilities** by accessing source and licence files, libraries, and their references in build configurations, checking them against its database. It also indicates updates for obsolete library versions, displaying project components and licences on the dashboard and in various reports.

Mend supports "developer integrations", making it easier for developers to identify and fix security and licensing issues from within their developer tools. It can seamlessly integrate with the development environment, building a pipeline to detect open source libraries with security or compliance issues. Mend reports severe software bugs, problematic licences, new versions and available fixes. It simplifies the management of open source libraries and the detection and remediation of compliance and security issues. Its database also includes public information provided by relevant external sources that report on software vulnerabilities. Mend builds an **inventory of software components** by detecting declared dependencies, matching them with a rich database providing **licence information**, warnings about outdated or risky open source libraries, and details of associated security vulnerabilities and issues. The provided licence information includes licence type, risk level, handling of patents, summary descriptions, and excerpts from original licence texts, etc. This helps to ensure compliance with organisations' licensing policies, and legal and security requirements, and that the components used are of high quality, secure, and up to date. However, Mend's licensing analysis and reports primarily target commercial organisations managing IPR risks posed by their assets. Also, it does not cover licence selection, compatibility,

and the compliance verification and management of licences of a large number of projects developed in the GÉANT projects.

Offered by WP9 Task 2, the Mend tool streamlines the process of verifying software IPR compliance and partially automates it. Mend provides visibility and control over the risks associated with open source. The licensing team sets up and maintains the Mend configuration, including the list of approved and rejected libraries provided by the software development team.

A short overview of Mend usage is available in the *Mend short guide for end users* [Wiki_MendGuide].

Mend can analyse projects in several ways. The provided code may be locally stored and a Mend scan can be manually triggered whenever the development team needs to assess the effects of a recent code change (details in *Adding project to Mend (Scan Flow)* [Wiki_MendAP]). Scanning of GÉANT software can be conducted by performing one integral Unified Agent (UA) project scan or multiple per-product scans. Currently, there is no versioning in Mend, so each software version is scanned as a separate Mend project.

Mend scans directories to find software components and identify vulnerable libraries, licensing conflicts or risks. After scanning the source code, it displays the results in the Mend web application. By default, it checks the digital signatures of used components in the Mend database to detect and describe open source or commercial components in the product. Mend is a platform that enables users to connect to a GÉANT product (without having to review the code) and assess its compliance with a predefined IPR policy. Verification is accomplished by scanning the project, populating the Mend web application dashboard with data about the project and enabling the creation of reports on compliance with the help of Mend's backend database.

The web-based GUI provides numerous options and panels for reviewing and analysing scans of open source software in an organisation's products and projects. Each scanned product or project is displayed on the corresponding page displaying summary information about a specific product or project and offering various dashboard options, providing a comprehensive view of the organisation's open source status. The product/project page provides access to all contained projects and libraries used by the product/project.

Each Mend dashboard segment leads to more detailed pages and reports with charts and tables. The dashboard displays the following information:

- **Product Alerts** – displays valuable information about library (component) alerts generated for a product. The **New Versions** category shows the number of alerts triggered for scanned libraries that are out of date (i.e., not the latest version). Whenever an out-of-date library is found, a new alert is generated and displayed in the **Alerts** report. The alert indicates the out-of-date library and its new version.
- **Security and Quality** – displays the number of libraries containing vulnerabilities, sorted by severity, the score of the most vulnerable library, the count of libraries with newer versions and vulnerabilities, and the count of "buggy" libraries.
- **Libraries** – presents detailed information about the product libraries (components), including library name, library licence, and per-product or per-project occurrences of libraries.
- **Licence Analysis** – provides data on the distribution of licences used by product or project components. It displays the number of different licence types.

Administrators can customise system settings, manage user permissions, and configure integration with third-party components. Additional and detailed information on licences is available in reports available from the Report menu. The Risk Report contains useful information for analysis and is the most detailed in terms of content. It is a tool that provides a view of all aspects of libraries, their licences, security and quality. The report contains several panels and tables displaying risk-related information. Security and licence analysis data is also presented in other parts of Mend, such as the Product Dashboard.

The displayed information is based on an internal database of libraries, their obsolete versions and vulnerabilities, licences and licence conflicts. Since this database is continually updated, the produced reports can change over time even if a scan has not been performed in the meantime, but this typically does not significantly impact overall licence risk numbers, as the most common licences are already covered well. It is worth repeating the scan as some changes in libraries and improvements in the Mend information about less common licences can significantly affect licence-related decisions during software licence analysis (SLA). Also, before scans are further improved by Mend, their results should be manually reviewed before conclusions about scanned software are drawn.

Mend information on OSS licences includes licence type, copyright, handling of patents and royalties, linking requirements, and compliance with free and open source software norms. Mend's experts have conducted an analysis of many licence types and defined risk scores to help developers assess risks associated with a particular licence. The primary score is the Copyright risk score calculated based on several factors (Risk Score Attribution [Mend_RSA]). Its purpose is to quantify, on a linear scale, the degree of loss of exclusive control over the code using a library or source code governed by that licence. The Copyright risk score is, therefore, more suitable for commercial organisations wanting to quantify or audit the level of exclusivity over their software assets and associated risks than it is for a software project willing to share, or interested in sharing, the code they developed. Since low values of this score, associated with the colour green, generally correspond to permissive licences, while high values, associated with red, correspond to strong copyleft licences, it can be used to quickly identify and assess the present licences. Licences are also quantified in terms of copyleft (no, partial, full) and linking (non-viral, dynamic, viral). There is also a Patent and Royalty risk score and a related attribute that indicates whether the software under the described licence is royalty-free (yes, conditional, no). Mend's Risk Report [Mend_TRR] provides a summary of the various risks detected.

Mend can integrate with development environments and build tools. It can be incorporated into a continuous integration (CI) pipeline, triggering scans with each commit in host repositories such as GitHub [GitHub], GÉANT GitLab [GN_GitLab] and Bitbucket [GN_Bitbucket]. GÉANT already uses Bamboo [GN_Bamboo] as the CI/CD software between the host repository and Mend (details in *Automated Mend scans with Bamboo* [Wiki_MendASB]).

Mend's functionality, originally tailored for commercial organisations and projects, is gradually moving towards licence compatibility checks more suitable for use within OSS projects. However, developers and project leaders still need to familiarise themselves with it and licence peculiarities and limitations.

Mend does not provide full and entirely accurate licence detection. It may report licences as unsolved or suspicious, or not use Software Package Data Exchange (SPDX) identifiers or full licence names. It may also use different names for the same or similar licences, or report licences without version numbers, which is particularly relevant for the GNU General Public License (GPL) as its various versions have different compatibility. These ambiguities affect the assessment of licensing risk and compatibility. Although the tool detects hundreds of licences, many are not detailed in its database. Such situations need manual investigation before a final decision on the product's licence is made. It is possible to manually correct licences of individual components at the organisational level. This helps with some libraries that do not have licence information or do not have a licence version specified. Sometimes, only suspect licences are indicated and they must be verified. Multi-licences and allowed relicensing are not always reliably handled and not all allowed licences are always listed. Mend currently does not provide a clear interpretation of dual-licensed or multi-licence libraries. It does report multiple licences, but this information often adds noise to the reports. For example, dual or multi-licensing with a high or medium-risk licence may raise an alarm due to the most restrictive licence, even if a more permissive alternative could also be applied. Also, there is no support for software versioning or differential reports.

All this prevents fully automated licence control and alerts. However, although effort to interpret and improve the Mend analysis is sometimes needed, its use is much more efficient than manual analysis. Even after it completes its composition analysis work, some decision-making and remediation are needed.

This is why the software licence analysis service described in Section 4.3 is needed. Mend provides a licence compatibility analysis indicating the (likely) compatibility of other components with the selected one. However, this is far from an automatic licence selection, which will probably always require human decision-making and trade-offs.

It should be noted that other tools can be used in software composition and licence analysis; some are listed in *Other software composition analysis (SCA, software inventory) tools* [Wiki_OtherSCATools] and in Section A.2 below. Mend is accurate compared with other tools tried by the OSLS team, as well as reports from other tools and internal documentation of dependencies provided by developers. It also fares better than other SCA tools in available comparative analyses. The problems that are experienced during its use are shared by other tools.

Mend supports the SPDX Software Bill of Materials (SBOM) format [Mend_SBOM], allowing the sharing of information about software product components between different tools. However, this is not yet fully useful because the licence identifiers used are the same as those in Mend's licence database and are often not recognised by other tools.

In practical use within GÉANT, Mend detected security vulnerabilities in libraries of several projects. In a significant portion, but not a majority of scans, it detected some high-severity security vulnerabilities. A few products with a large number of high-severity vulnerabilities are good candidates for targeted security analysis. Mend's mechanisms for finding security vulnerabilities still cannot fully replace other security-related tools, practices, and procedures.

The Mend company is developing Static Application Security Testing (SAST), which may bring a more granular security analysis that will also include detection of issues in new source code and not only in dependencies. It could be potentially used for security analysis together with or instead of SonarQube.

## A.2 Other SCA Tools and Resources

While Mend provides a variety of features for identifying, describing, and analysing licences, as well as an extensive database of libraries and licences, it is not always able to identify and describe libraries and licences correctly. Therefore, GÉANT will continue to explore other SCA tools, as well as services and other tools that can complement or possibly replace Mend in the future, especially those related to software licence analysis (and licence selection), to facilitate work that is not fully supported by Mend and to enrich the range of software tools available to developers, licence reviewers, and anyone responsible for IPR.

There are several commercial SCA tools and services. The advantage of using such tools is that, due to their commercial nature, they tend to be kept up to date, which is not always the case with freely available platforms.

- The GitLab Ultimate licence compliance feature is available for GitLab instances that include the GitLab Ultimate licence. It is directly integrated into the GitLab user interface and can be easily integrated into GitLab-managed CI/CD pipelines [GitLabLicense].
- FOSSA Open Source License Compliance Manager and Open Source Vulnerability Scanner [FOSSA1].
- Black Duck Software Composition Analysis [BlackDuck].
- JFrog Xray, an add-on for Artifactory [JFfrog].
- Snyk, a developer-first security platform for detecting security and code vulnerabilities in code, dependencies, containers, and infrastructure as code [Snyk], enabling developers to fix those issues early.
- Endor Labs products for exploring and managing OSS and working with SBOMs [EndorLabs].

There are also OSS tools that primarily perform SCA:

- OSS Review Toolkit [ORT].
- Projects in Python: pip-licenses [PIP], which dumps the software licence list of Python packages installed with pip.
- LicenseFinder finds dependencies and licences using package manager data for projects in Ruby, Python, Node.js, Bower, Nuget, Golang, and Java [LicenseFinder].
- The SPDX SBOM Generator creates SBOMs from package manager or build system data [SPDXSBOM].
- The Tern SCA tool and Python library generate an SBOM for container images and Docker files [Tern].
- FOSSology open source licence compliance software system and toolkit [FOSSology].
- ScanCode toolkit detects licences, copyrights and dependencies by scanning code to discover and inventory open source and third-party packages [ScanCode].
- The License Compliance Verifier (LCV) is a demonstrator based on a subset of the compatibility rules from the Open Source Automation Development Lab (OSADL) matrix [LCV].
- SQAaaS (Software Quality Assurance as a Service) checks for the presence of a LICENSE file with an OSI-approved licence as a part of a more extensive quality analysis (however, only compliance with the OSI Open Source Definition is required) [SQAaaS].
- License Maven Plugin manages the licence of a maven project and its dependencies [LMP].

The IPR Coordinator and WP9 Task 2 will review other SCA tools and their suitability for the GÉANT project.

There are also other resources which may help with licence selection:

- The “Choose an open source license” site provides excellent simple guidance on selecting various types of open source licences [Choose1]. Permissive licences are those which do not include the Same License condition [Choose2].
- The Joinup Licensing Assistant finds and compares software licences [JLA].
- The Open Source Guides site provides general resources and guides for getting started with OSS [OSG]. It also includes an excellent overview of the legal aspects of using OSS [OSGLegal].
- Creative Commons (CC) provides an online licence chooser for their licences [CC].
- The License Clearance Tool (LCT) by NI4OS-Europe suggests appropriate licences for open source and open source products, artefacts, and research results, based on manual entry of in-licences [LCT].
- Catalogue of standardised SPDX licence codes with licence texts [SPDXOrg].
- FOSSA provides a useful set of articles about licence compliance, including an article about the Microsoft Public License (Ms-PL) [FOSSA1], [FOSSA3].
- tl;drLegal provides simple explanations and classification of OSS licences [tldrLegal].

# Appendix B WP9 Task 2 Reviews Feedback Form

This appendix reproduces the tables in the WP9 Task 2 software reviews feedback form that relate to OSLS. The complete form is available at [WP9T2_ReviewFB].

## Section 5. During the Software Review

**General Question**

| | | | | Additional Information |
|---|---|---|---|---|
| 1 | Did you feel that you and your team were well-guided by WP9 T2 representatives? | ☐ Yes | ☐ No | |
| 2 | Did you feel that all significant details were consistently and adequately communicated between your developers and WP9 T2 reviewers? | ☐ Yes | ☐ No | |
| 3 | Please provide additional comments and recommendations that will help us get better during reviews. | | | |

**Software Composition Analysis (Type 3)**

| | | | | Additional Information |
|---|---|---|---|---|
| 1 | Has Mend provided you with sufficient information to address the licensing issues or vulnerabilities? | ☐ Yes | ☐ No | |
| 2 | If 'No', how would you prefer to learn more about the issue? | ☐ Search on Internet<br>☐ Mend help<br>☐ Materials from the Software Licence Management (SLM) team<br>☐ Contact the SLM team | | |

| | | | | Additional Information |
|---|---|---|---|---|
| 3 | What is your preferred way to communicate issues found by Mend during the review to your development team? | ☐ Mend report<br>☐ Jira tickets<br>☐ Slack communication<br>☐ Email (referencing the Jira ticket)<br>☐ Other | | If there is another way that would suit you, please mention it here: |
| 4 | Do you think the issues reported by Mend are strict, reasonable or loose? | ☐ Strict<br>☐ Reasonable<br>☐ Loose | | |
| 5 | Have you found any false positives in Mend or other detected issues you are not convinced about? | ☐ Yes | ☐ No | If 'Yes', explain briefly: |
| 6 | Have you identified any part of your project that, in your opinion, is within Mend's scope but Mend did not detect it? | ☐ Yes | ☐ No | If 'Yes', explain briefly: |
| 7 | Were there any existing Software Composition Analysis features that you found useful or liked? | ☐ Yes | ☐ No | If 'Yes', explain briefly: |
| 8 | Do you have any ideas about using Mend more effectively or other suggestions for Software Composition Analysis improvement? | Your ideas: | | |

**Software Licence Analysis (Type 4)**

| | | | | Additional Information |
|---|---|---|---|---|
| 1 | Has the Software Licence Management (SLM) team sufficiently explained licensing issues? | ☐ Yes | ☐ No | |
| 2 | If 'No', how would you prefer to receive clarifications? | ☐ Search on Internet<br>☐ Contact your colleague from the development team<br>☐ Contact the SLM team<br>☐ Receive references, links or examples | | |

| | | | | Additional Information |
|---|---|---|---|---|
| 3 | What is your preferred method for the SLM team to communicate issues found during the review to your development team? | ☐ PDF documents<br>☐ Jira tickets<br>☐ Slack communication<br>☐ Email (referencing the Jira ticket)<br>☐ Other | | If there is another way that would suit you, please mention it here: |
| 4 | Are there reported issues that could not be addressed due to software architecture or that are too challenging to correct? | ☐ Yes | ☐ No | If 'Yes', explain briefly: |
| 5 | Are there any reported issues you disagree with and remain unconvinced about? | ☐ Yes | ☐ No | If 'Yes', explain briefly: |
| 6 | Do you think the issues reported by the SLM team are strict, reasonable or loose? | ☐ Strict<br>☐ Reasonable<br>☐ Loose | | |
| 7 | Were there any existing Software Licence Analysis features that you found useful or liked? | ☐ Yes | ☐ No | If 'Yes', explain briefly: |
| 8 | Do you have any ideas about using Software Licence Analysis more effectively or other suggestions for its improvement? | Your ideas: | | |

# References


| | |
|---|---|
| [BlackDuck] | https://www.synopsys.com/software-integrity/security-testing/software-composition-analysis.html |
| [BP] | https://wiki.geant.org/display/GSD/Catalogue+of+best+practices |
| [CC] | https://creativecommons.org/choose/ |
| [Choose1] | https://choosealicense.com/ |
| [Choose2] | https://choosealicense.com/licenses/ |
| [Contact] | Email: sw-licences@software.geant.org<br>Slack: #sw-licences in geant-project.slack.com workspace |
| [GN4-3_D9.2] | https://geantprojects.sharepoint.com/sites/gn4-3/Work-Packages/WP9/Deliverables%20Documents/Software%20Policy/GN4-3_D9.2-Software-Policy.pdf<br>Note that this document is classed as confidential and can, therefore, only be viewed by project participants |
| [Dillinger] | https://dillinger.io/ |
| [eduTEAMS] | https://eduteams.org/ |
| [EndorLabs] | https://www.endorlabs.com/ |
| [EURISE_SQC] | https://technical-reference.readthedocs.io/en/latest/quality/software-checklist.html |
| [Evaluation_Survey] | https://wiki.geant.org/display/gn51wp9t2/Evaluation+Survey |
| [FOSSA1] | https://fossa.com/product/open-source-license-compliance |
| [FOSSA2] | https://fossa.com/product/open-source-vulnerability-management |
| [FOSSA3] | https://fossa.com/blog/open-source-licenses-101-microsoft-public-license-ms-pl/ |
| [FOSSology] | https://www.fossology.org/ |
| [GA] | https://connect.geant.org/2022/11/08/a-new-ipr-policy-for-the-geant-project-*connect*-interview-with-magdalena-rzaca-gdpr-ipr-legal-advisor-at-geant |
| [GitHub] | https://github.com/ |
| [GitLabLicense] | https://docs.gitlab.com/ee/user/compliance/license_compliance/ |
| [GN_Bamboo] | https://bamboo.software.geant.org/ |
| [GN_Bitbucket] | https://bitbucket.software.geant.org/repos?visibility=public |
| [GN_BP_B6] | https://wiki.geant.org/display/GSD/BP-B.6%3A+Manage+sideground+IPR |
| [GN_GitLab] | Community Edition instance, hosting most projects: https://gitlab.software.geant.org/public<br>Ultimate Edition, hosting a few selected projects: https://gitlab.geant.org/ |
| [GN_IPRPolicy] | https://resources.geant.org/wp-content/uploads/2022/09/GEANT-_IPR_Policy_2022.pdf |
| [GN_Resources_IP] | https://resources.geant.org/publications/intellectual-property/ |
| [GN_SC] | https://sc.geant.org/ |
| [GPS2023_LT] | https://wiki.geant.org/pages/viewpage.action?pageId=661521647 |
| [GPS2023_SB] | https://wiki.geant.org/display/gn51wp9t2/Deep+dive+into+Software+Governance+-+quality+badges |
| [HelpDesk] | https://jira.software.geant.org/servicedesk/customer/portal/2/create/55 |
| [InfoShareGuides] | https://wiki.geant.org/display/gn51wp9t2/Infoshare%3A+OSS+Licensing+and+Licence+Compliance+Guidelines+for+Software+Developers |
| [InfoSharePolicy] | https://events.geant.org/event/1314/ |

| | |
|---|---|
| [IntroOSLC_Training] | https://e-academy.geant.org/moodle/course/view.php?id=478 |
| [IPRSupport] | iprcoordinator@geant.org |
| [IPRUpdate] | https://wiki.geant.org/display/UIP/Update+of+IPR+Policy+Home |
| [JFfrog] | https://jfrog.com/xray/ |
| [Jira_RSWR] | https://jira.software.geant.org/servicedesk/customer/portal/2/create/55 |
| [JLA] | https://joinup.ec.europa.eu/collection/eupl/solution/joinup-licensing-assistant/jla-find-and-compare-software-licenses |
| [KB] | https://wiki.geant.org/display/GSD/Knowledge+Base |
| [LCT] | https://lct.ni4os.eu/ |
| [LCV] | https://github.com/fasten-project/fasten/wiki/License-compliance |
| [LDAwithWS_Webinar] | https://e-academy.geant.org/moodle/course/view.php?id=220<br>https://wiki.geant.org/display/gn43wp9/Webinar%3A+Licence+Analysis+with+WhiteSource |
| [LicenseFinder] | https://github.com/pivotal/LicenseFinder |
| [LMP] | Introduction: https://www.mojohaus.org/license-maven-plugin/index.html<br>GitHub: https://github.com/mojohaus/license-maven-plugin |
| [Make_a_README] | https://www.makeareadme.com/ |
| [Mend_RSA] | https://docs.mend.io/bundle/sca_user_guide/page/understanding_risk_score_attribution_and_license_analysis.html#Risk-Score-Attribution |
| [Mend_SBOM] | https://www.mend.io/blog/guide-to-standard-sbom-formats/ |
| [Mend_SCA] | https://www.mend.io/sca/ |
| [Mend_TRR] | https://docs.mend.io/bundle/sca_user_guide/page/the_risk_report.html |
| [ORT] | https://github.com/oss-review-toolkit/ort |
| [OSG] | https://opensource.guide/ |
| [OSGLegal] | https://opensource.guide/legal/ |
| [OSI_Licences] | https://opensource.org/license |
| [OSLC_Training] | https://e-academy.geant.org/moodle/course/view.php?id=214 |
| [OSRB] | https://wiki.geant.org/pages/viewpage.action?pageId=633276009 |
| [Pack] | https://wiki.geant.org/display/GW/GN5-1+and+GN5-IC1+Onboarding+Presentations+and+Guidance |
| [PIP] | https://pypi.org/project/pip-licenses/ |
| [PLM] | https://geantprojects.sharepoint.com/sites/plm |
| [RedHat_COSP] | https://www.redhat.com/en/resources/open-source-project-health-checklist |
| [SC] | https://sc.geant.org |
| [ScanCode] | https://github.com/nexB/scancode-toolkit |
| [SideIPR] | https://wiki.geant.org/display/GSD/BP-B.6%3A+Manage+sideground+IPR |
| [Snyk] | https://snyk.io/ |
| [SPDXOrg] | https://spdx.org/licenses/ |
| [SPDXSBOM] | https://github.com/opensbom-generator/spdx-sbom-generator |
| [SQAaaS] | https://sqaaas.eosc-synergy.eu/ |
| [StackEdit] | https://stackedit.io/ |
| [SWLMinGN_Infoshare] | https://wiki.geant.org/pages/viewpage.action?pageId=633276866 |
| [SLS&MG] | GN5-1 white papers: https://resources.geant.org/wp-content/uploads/2024/04/GN5-1_Software-Licence-Selection-and-Management-in-GEANT.pdf<br>Zenodo: https://doi.org/10.5281/zenodo.10907564 |
| [Tern] | https://github.com/tern-tools/tern |
| [TinyMCE_OSSEC] | https://www.tiny.cloud/software-evaluation-criteria-checklist/ |
| [tldrLegal] | https://tldrlegal.com/ |
| [Wiki_CGSCA] | https://wiki.geant.org/pages/viewpage.action?pageId=599785535 |
| [Wiki_ImportantLicences] | https://wiki.geant.org/display/GSD/Important+licences+for+licence+selection |

[Wiki_MendAccess] https://wiki.geant.org/display/gn51wp9t2/Accessing+Mend+and+visibility+levels
[Wiki_MendAP] https://wiki.geant.org/pages/viewpage.action?pageId=240844905
[Wiki_MendASB] https://wiki.geant.org/pages/viewpage.action?pageId=219938818
[Wiki_MendGuide] https://wiki.geant.org/display/GSD/Mend+short+guide+for+end+users
[Wiki_OSSL&LS] https://wiki.geant.org/display/GSD/OSS+licences+and+licence+selection
[Wiki_OSSL_RefInfo] https://wiki.geant.org/display/GSD/Reference+information+about+OSS+licences+and+tools
[Wiki_OSSLWP] https://wiki.geant.org/pages/viewpage.action?pageId=633275197 [federated login required]
[Wiki_OtherSCATools] https://wiki.geant.org/display/GSD/Reference+information+about+OSS+licences+and+tools#ReferenceinformationaboutOSSlicencesandtools-Othersoftwarecompositionanalysis(SCA,softwareinventory)tools
[Wiki_SCT] https://wiki.geant.org/display/GSD/Secure+Code+Training
[Wiki_SWReviews] https://wiki.geant.org/display/GSD/Software+Reviews
[WP9T2_ReviewFB] https://wiki.geant.org/pages/viewpage.action?spaceKey=gn51wp9t2&title=Evaluation+Survey

# Glossary

| | |
|---|---|
| **AGPL** | GNU Affero General Public Licence |
| **API** | Application Programming Interface |
| **Artifactory** | An artefact repository manager |
| **BSD** | Berkeley Software Distribution |
| **CC** | Creative Commons |
| **CC BY** | Creative Commons Attribution licence |
| **CC BY-NC** | Creative Commons Attribution-NonCommercial licence |
| **CC BY-ND** | Creative Commons Attribution-NoDerivs licence |
| **CD** | Continuous Delivery |
| **CDDL** | Common Development and Distribution License |
| **CI** | Continuous Integration |
| **CI/CD** | Continuous Integration / Continuous Delivery |
| **EC** | European Commission |
| **eduGAIN** | GÉANT service that provides an efficient, flexible way for participating federations, and their affiliated users and services, to interconnect |
| **eduTEAMS** | GÉANT service that enables members of the R&E community to create and manage virtual teams and securely access and share common resources and services using federated identities from eduGAIN and trusted identity providers |
| **EU** | European Union |
| **EUPL** | European Union Public Licence |
| **EURISE** | European Research Infrastructure Software Engineers |
| **FAIR** | Findability, Accessibility, Interoperability and Reusability |
| **fauxpen** | A term combining “faux” and “open” which, like source available, refers to a type of non-OSS restrictive proprietary licence often presented or perceived as similar to OSS |
| **FoD** | Firewall on Demand |
| **FOSSA** | An open source risk management platform |
| **GLAD** | GÉANT Learning and Development |
| **GN4-3** | GÉANT Network 4 Phase 3, a project part-funded by the EC’s Horizon 2020 programme under Specific Grant Agreement No. 856726 |
| **GN5-1** | GÉANT Network 5, Phase 1, a project funded by the European Union’s Horizon Europe research and innovation programme under Grant Agreement No. 101100680 and one of the projects implementing the actions defined in the GN5 Framework Partnership Agreement |
| **GPL** | GNU General Public License |
| **GUI** | Graphical User Interface |
| **ICT** | Information and Communication Technology |
| **InAcademia** | GÉANT service providing real-time, secure validation of student affiliation |
| **IP** | Intellectual Property |
| **IPR** | Intellectual Property Rights |
| **ISC** | Internet Software Consortium |
| **KPI** | Key Performance Indicator |
| **LCT** | License Clearance Tool |
| **LCV** | License Compliance Verifier |
| **LGPL** | GNU Lesser General Public License |

| | |
|---|---|
| **Maat** | A tool for managing information about infrastructure resources and services in network automation and orchestration use cases (formerly Inventory3) |
| **MIT** | Massachusetts Institute of Technology |
| **MS** | Microsoft |
| **Ms-PL** | Microsoft Public License |
| **NI4OS** | National Initiatives for Open Science in Europe |
| **NMaaS** | Network Management as a Service |
| **NREN** | National Research and Education Network |
| **OS** | Operating System |
| **OSADL** | Open Source Automation Development Lab |
| **OSI** | Open Source Initiative |
| **OSLS** | Open Source and Licence Support |
| **OSRB** | Open Source Review Board |
| **OSS** | Open Source Software |
| **PLM** | Product Lifecycle Management |
| **R&E** | Research and Education |
| **SaaS** | Software as a Service |
| **SAST** | Static Application Security Testing |
| **SBOM** | Software Bill of Materials |
| **SCA** | Software Composition Analysis |
| **SHBPRFL** | User Profile Page plugin for Shibboleth |
| **SLA** | Software Licence Analysis |
| **SLM** | Software Licence Management |
| **SonarQube** | An open source platform for continuous inspection of code quality |
| **SPDX** | Software Package Data Exchange |
| **SQAaaS** | Software Quality Assurance as a Service |
| **SSO** | Single Sign-On |
| **SSPL** | Server Side Public License |
| **T&I** | Trust and Identity |
| **TCO** | Total Cost of Ownership |
| **TimeMap** | GÉANT open source latency/jitter measurement service |
| **UA** | Unified Agent |
| **UI** | User Interface |
| **URL** | Uniform Resource Locator |
| **VAaaS** | Vulnerability Assessment as a Service |
| **WP** | Work Package |
| **WP5** | Work Package 5 Trust & Identity Services Evolution and Delivery |
| **WP9** | Work Package 9 Operations Support |
| **WP9 Task 2** | WP9 Task 2 Software Governance and Support |