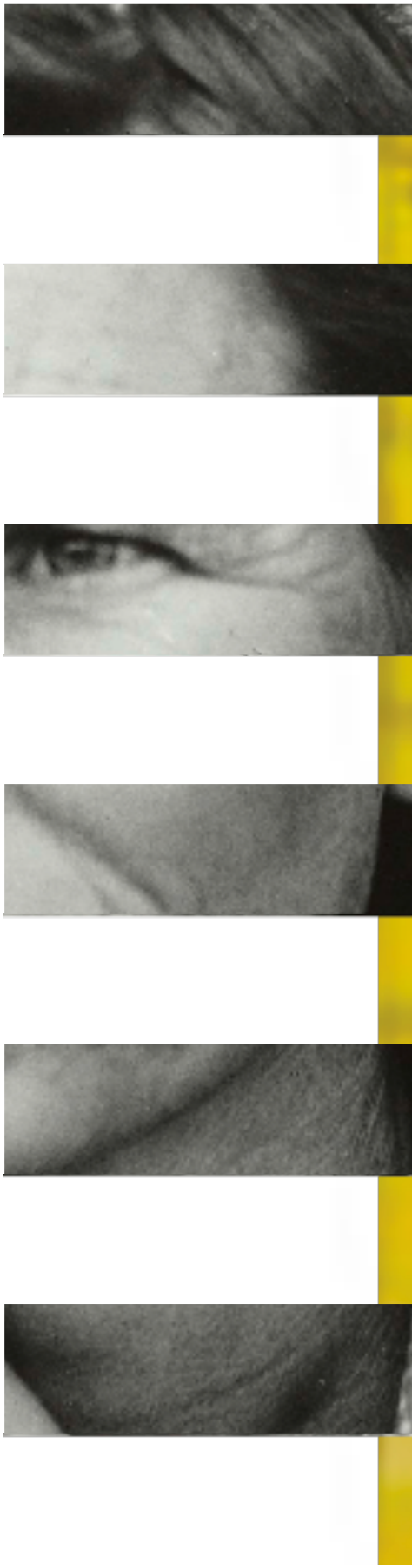


CommonsDB feasibility study

Part 1

June 2025

Authors

Paul Keller, **Doug McCarthy** Open Future,

Sebastian Posth Liccium - Chapter 3,

João Pedro Quintais, **Kacper Szkalej**, **Thomas Margoni**

Institute for Information Law - Chapter 4

commons DB

CommonsDB is an initiative funded by the European Commission to develop and test a prototype registry of Public Domain and openly licensed works. CommonsDB is led by Open Future in collaboration with Liccium, Europeana Foundation, Wikimedia Sverige, and the Institute for Information Law (IViR).

This study has been co-funded by the European Union under the 2023 work programme on the financing of Pilot Projects and Preparatory Actions in the field of Communications Networks, Content and Technology. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or European Commission. Neither the European Union nor the European Commission can be held responsible for them.

Contents

1

Introduction

This is the first part of two parts of a feasibility study for a public registry of public domain and openly licensed works. This registry – called CommonsDB – is currently being developed by a consortium consisting of Open Future, Liccium, the Institute for Information Law, Europeana Foundation, and Wikimedia Sweden as part of a European Commission-funded pilot project running from 1 February 2025 to 31 July 2026.

The present first part of the feasibility study has been undertaken in parallel with the initial stages of development of the prototype registry. As such, it is not a traditional feasibility study that examines the technical and conceptual feasibility of building a registry prior to its implementation.

Instead, the first part of the feasibility study describes and scopes the system that is being developed, including but not limited to the objectives, parameters (section 2), and the technological approach (section 3). Based on this analysis the study also provides a detailed legal analysis of the proposed approach with a special focus on copyright law (section 4). Finally, the study also identifies technical, operational, and legal issues that will need to be addressed as part of building the prototype (section 5).

The second part of the feasibility study (to be delivered in November 2025) will explore these issues in greater detail with the objective of presenting solutions that can be incorporated in the final version of the prototype that we expect to deliver in the first quarter of 2026.

The main objective of the present study is to make our development approach and design decisions transparent and to enable stakeholder feedback.

2

Objectives

The overall objective of the CommonsDB initiative is to build and test a prototype of a public registry for public domain and openly licensed works that can bring greater legal certainty to the reuse of digital content. In this section we will zoom into some of the core concepts embedded in this objective.

What do we mean when we say ‘registry’?

The concept for CommonsDB was conceived in response to a call for proposals for a EU repository of public domain and open licensed works. The distinction between the two terms – repository and registry – is an important one when it comes to understanding the objective, the choice of technological approach, and the scope of the work that we are undertaking as part of the CommonsDB initiative.

Our proposal to build a registry (a system that maintains rights information and other metadata) instead of a repository (a system that stores digital copies together with their metadata) is based on the realization that what is needed to achieve the core objective – increasing legal certainty around the use of openly licensed and public domain works – is not to build another repository of such works but rather a registry of verifiable rights information. There are already a number of repositories for public domain and openly licensed works. Wikimedia Commons, which contains more than 117 million digital files, is the most widely used repository of such content. In addition, there are many other systems – including Europeana – that serve as repositories and that contain public domain and openly licensed works. In addition, there are a number of commercial platforms that contain significant amounts of openly licensed and public domain works and that can be seen as repositories as well. As a result of the fact that works that are openly licensed or in the public domain can be shared without any restrictions, there is a large degree of overlap when it comes to the works contained in different repositories.

Our approach to creating more legal certainty is not based on an attempt to build another repository that would aggregate works and metadata contained in different repositories, as this means that we have to invest in replicating already existing functionality. It is also very likely that such an approach would be perceived as competition by existing repositories and the communities that exist around them – communities that we need to be supportive of for our approach to succeed.

What we are proposing instead is to build a registry that brings together rights information about public domain and openly licensed works contained in existing repositories in a single registry with a narrowly defined focus on rights binformation. CommonsDB will be architected so that it can function as a clearing house for rights information, and we envisage it as providing an interoperable rights information service that stores rights information separate from the actual works.

This approach also informs the functionality of what we are building, especially when it comes to end-user-facing functionality. While the technical underpinnings allow us to store and make available a wide spectrum of metadata associated with digital works, we will deliberately limit the information that will be stored within the system to information that is necessary for the core functionality: looking up and verifying rights information related to public domain and openly licensed works. **This also means that we are not planning to build a (meta) search engine for public domain or openly licensed works. We are not intending to compete with the discovery services provided by existing repositories but rather intend to complement them, by enabling users to trace works back to them.**

What do we mean when we say ‘works’?

In this context, it is important to highlight a conceptual limitation of our approach. While our objective is to build a registry of public domain and openly licensed works, the attachment mechanism we are using to connect rights information applies to specific manifestations of works in the form of digital assets. This means that technically, we are building a registry that contains rights information about manifestations of works in concrete digital files and not the intangible object (corpus mysticum) as such.

The ISCC codes that are at the core of our technical implementation are content identifiers that are derived from specific digital assets, and while they are capable

of signaling similarity between assets, they cannot automatically determine that two different manifestations of the same work belong to the same work. Understanding how similarity scores between ISCC codes can be leveraged to achieve this will be an important part of the testing and validation of the prototype, but it is important to realize that identifying works (in the abstract sense of the concept that underpins copyright) is not a primary objective of the CommonsDB infrastructure. There are existing approaches (persistent work identifiers) that serve this purpose and that can be integrated into the functionality of the CommonsDB prototype.

What do we mean when we say ‘public domain and openly licensed’?

CommonsDB is not a generic rights information service. Instead, we are focusing on digital assets that are either in the public domain or that are openly licensed. The registry is technically capable of storing rights information of any sort (including about digital assets that are in copyright but not available under open licenses), but in line with the objective, it will be designed to only contain information about digital assets that can be reused without any restrictions in line with the Open Definition (see the next section for more details on how this will be operationalized).

What do we mean when we say ‘prototype’?

During the current phase, which concludes on 31 July 2026, our efforts will center on building and validating a prototype registry. The purpose of this prototype will be to test our conceptual approach, understand its limitations, validate the usefulness of the concept, and test the technological implementation at scale. CommonsDB will be developed on a set of existing technological building blocks and standards and requires relatively little technological development from scratch. The main purpose of the prototype is to test the integration with data providers and to test the underlying technological building blocks at scale. By July 2026, our ambition is for the prototype registry to contain at least 5 million declarations from at least 5 different data partners.

While the underlying technological infrastructure is designed to be able to contain information to openly licensed and public domain works of any sort, we will initially operate and test the prototype with visual works (images). We intend

to integrate other media types once we have successfully demonstrated the functionality with rights information related to images. It is our ambition to integrate information for at least one other media type during the prototype phase – most likely video.

What do we mean when we say ‘greater legal certainty’?

Ultimately, CommonsDB seeks to solve two key problems related to the management of rights information for openly licensed and public domain works that are available online. In the current situation, rights information lacks strong connections with the digital assets that it applies to. Rights information and other metadata are generally stored either alongside the assets or as embedded metadata and easily get lost when these assets circulate online. In addition, there are currently no well-established mechanisms for verifying the identity of entities that issue licenses or make declarations related to the public domain status of digital assets. Without reliable information about the identity of such entities, it is often difficult to assess if rights information can be relied on or not.

1. CommonsDB will build mechanisms that enable stronger relationships between digital assets and their associated rights information. The setup that we are proposing will allow anyone to obtain this information based on the assets themselves without having to rely on the presence of metadata. This mechanism will also make it possible to enable more reliable attribution of parties such as cultural heritage institutions that make collections available online.

2. The same mechanisms will also create more legal certainty by creating strong, verifiable links between rights information and the entities that make assertions about the copyright status or licensing conditions of digital assets that they make available online.

The focus on these two problems will drive the overall design of the registry. The functionality provided by CommonsDB will be focussed on additional capabilities that augments existing repositories of public domain and openly licensed works, instead of replicating existing capabilities.

2.1 Design principles

Our approach to building CommonsDB is based on three design principles. (1) CommonsDB will be based on existing standards, (2) the CommonsDB registry will be built with the ability to function as part of a federated network of registries, and (3) we will strive for maximum openness.

2.1.1 Standards-based

Key technological building blocks for CommonsDB are based on existing standards. Central to our approach is the use of ISCC codes (ISO 24138) and verifiable credentials. The concept for Commons DB is only possible because of the existence of the ISCC standard. Building on top of this standard enables us to bind the rights information to digital assets in a way that it can be retrieved by anyone who has access to the media file. This is possible because the ISCC is based on a publicly documented standard that enables anyone to create ISCC codes that can be used as a lookup key for the rights information. ISCC works for a wide range of media types and file formats, making it an ideal candidate for implementing CommonsDB.

In addition, CommonsDB will make use of Verifiable Credentials in order to ascertain the identity of entities (declaring parties) that submit declarations into the registry. These credentials will be supported by advanced and qualified certificates, compliant with the eIDAS regulation, to accurately identify content partners or trust services that certify the parties involved.

2.1.2 Federation

While we are developing the registry component of the prototype as a single stand-alone instance, it will be architected with federation as a core design principle. Federation is essential for scalability, resilience, and long-term inter-operability with other registries operated by third parties. The architecture will support a distributed network of registries that can synchronize metadata records using standardized protocols and identifier schemes.

In particular, we are exploring a hybrid approach combining centralized indexing (for search applications) with decentralized discovery mechanisms, including the use of Distributed Hash Tables (DHTs) for record lookup and resolution. This would allow participants to potentially maintain their own registries while contributing to a shared namespace. We plan to evaluate these federated approaches in more detail through the two use cases (AI training data and Article 17 compliance) in the second half of the project.

2.1.3 Openness

CommonsDB will be realized as a public registry; this means that all information that will be collected in the registry (and the associated Metadata Storage) will be public and will be available as open data. This approach is possible because for CommonsDB we are dealing with information (metadata) about digital assets that are either in the public domain or openly licensed.

The majority of metadata that we will be processing is free from copyright to begin with, and while there are some elements that may be protected by copyright (such as preview images), the fact that CommonsDB only contains information about digital assets that meet the open definition ensures that all data that we are processing can be made available as open data (for more details, see the legal analysis in section 4 of this study).

2.2 Implementation

2.2.1 Definition of public domain and openly licensed

To develop a functional registry of public domain and openly licensed works, it is essential to establish a clear conceptual understanding of these two concepts. In practical terms this comes down to making a selection which rights statements and licenses will be considered “open” and thus supported within the registry.

CommonsDB will support rights statements that irrevocably permit the free use, redistribution (including commercial redistribution), and modification of works, thereby enabling the creation and distribution of derivative works under the same terms. This approach is based on international open data standards such as the Open Definition.

Furthermore, all supported rights statements and licenses in CommonsDB must be machine-readable and interoperable, allowing computational systems to discover, access, interoperate with, and reuse data with minimal or no human intervention, consistent with the FAIR Principles.

Given their alignment with these principles and their widespread adoption, the Creative Commons licenses and Public Domain tools have achieved widespread global recognition and significant adoption across various sectors, including education, academia, media, and the arts, facilitated by their legally robust framework and the flexibility they offer creators. Millions of works, encompassing

images, music, videos, and educational resources, are licensed under CC licenses, with platforms such as Wikimedia Commons and Europeana hosting substantial amounts of CC-licensed content.

To ensure broad accessibility and interoperability within our registry, we will utilize the Creative Commons licenses and Public Domain tools as our foundational framework for recording rights information. This approach is driven by the widespread adoption of CC licenses within the open access community, including our data partners.

From the suite of CC licenses and Public Domain tools, we have identified the following four that meet the criteria of the Open Definition and will therefore be supported in the CommonsDB registry:

1. Public Domain Mark: This indicates that a work is no longer subject to copyright restrictions and can be freely used by others. Typically, the Public Domain Mark is applied to straightforward digital reproductions of works whose copyright has elapsed or never existed in the first place. This statement is in line with Article 14 of the 2019 Copyright in the Digital Single Market (CDSM) Directive, which defends the principle that public domain works should remain in the public domain when digitized.

2. CC0: This enables copyright (or database right) holders to waive their rights in their works, effectively placing them as fully as possible into the public domain. This allows others to freely build upon, enhance, and reuse the works for any purpose without restriction.

3. CC BY: This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, provided that attribution is given to the creator. This license also permits commercial use.

4. CC BY-SA: This license allows reusers to distribute, remix, adapt, and build upon the material in any medium or format, provided that attribution is given to the creator. This license also permits commercial use. If users remix, adapt, or build upon the material, they must license the modified material under identical terms.

Consequently, digital assets licensed under the more restrictive Creative Commons licenses that do not align with the Open Definition (i.e., those including Non-Commercial (NC) or No Derivatives (ND) restrictions) will not be accepted into the registry, because they do not qualify as openly licensed.

In principle, we will also consider accepting digital assets made available under compatible or equivalent rights statements or licenses, provided they meet our other technical requirements, such as machine readability. The necessity and implementation details for supporting such alternative statements will be evaluated in the later stages of the project.

Furthermore, to enhance the utility and context of Public Domain designations, where available the rationale behind why a work is marked as being in the public domain will be recorded. Documenting the rationale for a public domain determination provides valuable context for reusers, allows the external verification of determinations that have been made and will lead to a clearer understanding of the work's legal status. Explicit information about the rationale behind a public domain determination is being held by some repositories (Wikimedia Commons) while others (such as Europeana) generally do not record it. By including information about the rationale for public domain determinations in CommonsDB we aim to make this information more widely available.

2.2.2 Minimal reproduction and limited metadata

To achieve its core objective of providing verifiable rights information efficiently, CommonsDB will adhere to the principle of minimal reproduction, which in turn dictates a focus on limited but essential metadata.

Instead of replicating the extensive metadata already associated with the digital assets contained in existing repositories like Wikimedia Commons and Europeana, CommonsDB will primarily focus on the metadata directly relevant to establishing and verifying the open status of a work. This includes the specific rights statement or license (e.g., Public Domain Mark, CC0, CC BY), the ISCC code that uniquely identifies the digital asset, and the verifiable credentials of the declaring party. These will be stored in the actual CommonsDB Registry.

While Data Suppliers can include other useful metadata such as descriptions and publication dates in the Metadata Storage, the CommonsDB's core functionality hinges on the minimal set of data points necessary for rights verification (an overview of the metadata scheme for Data Supplier declarations to CommonsDB can be viewed in the Annex).

This approach avoids the complexities and potential inconsistencies of aggregating diverse metadata schemas from various repositories. By focusing on a limited and well-defined set of metadata, CommonsDB can ensure interoperability and efficient querying, supporting its aim of increasing legal

certainty for the reuse of public domain and openly licensed works. This streamlined approach also aligns with the principle of not competing with existing repositories but rather complementing their functionality by providing a focused layer of verifiable rights information.

3

Technical architecture

The CommonsDB registry will utilize a federated architecture for managing and distributing rights information about public domain and openly licensed works. It will leverage the International Standard Content Code (ISCC) as a key to exchange rights information about digital assets. This design will enable any third-party actor or system with access to a copy of the file to retrieve rights information using the ISCC code derived from the digital media file.

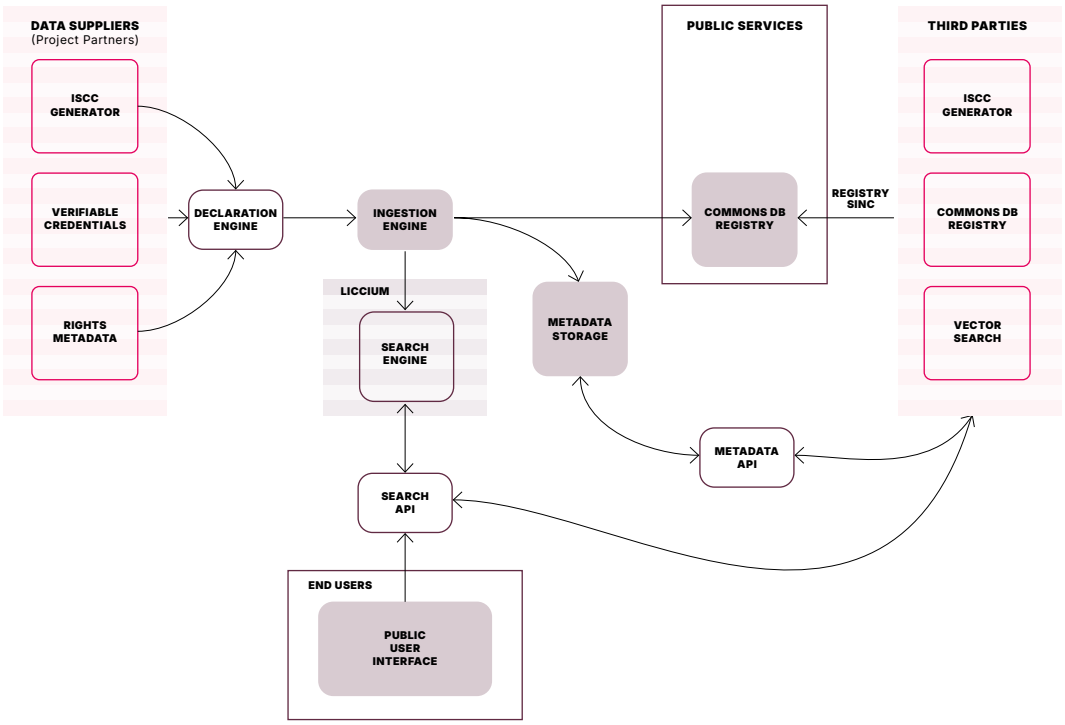
The prototype registry will serve as an open and accessible repository for ISCC codes, rights information and other metadata, and verifiable credentials from Data Suppliers, acting as a hub for rights information about public domain and openly licensed digital assets. In the future, we envisage a network of interconnected federated registries as a compromise between centralized and fully decentralized approaches.

3.1 Core infrastructure

The CommonsDB core infrastructure includes the following elements:

- **ISCC Generator:** Outputs International Standard Content Codes (ISCC) and technical metadata for content identification and tracking. The software is installed locally by Data Suppliers and Third Parties and provided as a service for the Public User Interface.

- **Declaration API:** The API through which Data Suppliers submit digitally signed metadata, such as ISCCs, Rights Metadata, and Verifiable Credentials, when making declarations to the registry.



CommonsDB technical overview (April 2025)

- **Ingestion Engine:** Processes and integrates declarations data from Data Suppliers. Its inputs include digitally signed data objects with ISCCs, rights statements, certificates or verifiable credentials. The Ingestion Engine writes a subset of declaration metadata into CommonsDB Registry.

- **Metadata Storage:** Stores full declaration metadata and content-related information from Data Suppliers for search and discoverability. It will output metadata objects based on calls of the Metadata API by third parties or platforms.

- **CommonsDB Registry:** The registry of public domain and openly licensed digital assets, containing a subset of machine-readable declaration meta-data from Data Suppliers.

- **Metadata API:** Provides programmatic access to the stored metadata for the purpose of third-party integrations.

- **Search API:** Enables third parties and the Public User Interface to query the metadata.
- **Public User Interface:** Enables users to interact with the registry. Users can query content, retrieve metadata, and upload media assets for search and verification.
- **Search Engine:** Indexes metadata to power search functionality to third parties and the Public User Interface.
- **Vector Search:** Enables querying for identical or similar ISCC codes using vector-based comparison.

3.1.1 International Standard Content Codes

A key feature of the registry architecture is the utilization of ISCCs (ISO 24138) for decentralized digital content identification. The ISCC is a new, open identification system and a published ISO standard that enables the identification of digital assets of all media types independently of where the content is available. With ISCC codes, any user or entity with access to digital media content can derive identifiers directly from digital media files that they process, host, or share. ISCC is a multi-composite identifier that combines cryptographic hashes to verify content integrity and determine whether a file has been modified, with similarity-preserving hashes in the other code units. This means that in cases where there are different versions of the same content or content in different file formats, slightly modified or manipulated content, or content from which the metadata has been removed, the identifiers derived from the content will be different but likely to match up to a certain level of modification, supporting the efficient detection of near-duplicates while ensuring content integrity.

Already today, ISCC codes can be generated from most file formats of all media types, such as text, images, video, and audio, allowing the same identification system to be used across all media sectors and content types. Because the ISCC is generated directly from the digital media file, there is no need to manually apply and manage the identifier. Each digital media file has – metaphorically speaking – its own unique DNA that is extracted from the content. This means that two users (or machines) who do not need to know or trust each other can generate the same or a similar identifier directly from the media file without exchanging any information or metadata about the content. ISCC's unique characteristics solve a major problem in digital distribution by eliminating the need for manual identifier management and addressing the challenge of identifying content online where metadata is often lost.

3.1.2 Verifiable Credentials

To ensure the authenticity of metadata records and the identity of the Data Suppliers submitting declarations, CommonsDB incorporates Verifiable Credentials (VCs) as a core trust mechanism. By using VCs, the registry ensures a consistent and interoperable way to verify who made a declaration. Declarations submitted to the registry are digitally signed using cryptographic key material controlled by each Data Supplier. This guarantees the integrity of the declaration and its binding to the declaring party. The VCs associated with these signatures conform to the W3C standard for Verifiable Credentials and are compatible with the eIDAS-compliant framework. This structure allows any third party to cryptographically verify the identity of a declaration's originator, even without interaction between parties or any manual verification process.

The CommonsDB registry will adopt a hierarchical trust model in which the project coordinator Open Future – fully certified and operating in compliance with EU trust standards – functions as an issuer of Verifiable Credentials to Data Suppliers. These credentials will link public keys to verified organizational identities. Once issued, the VC will be attached to each declaration and published alongside the ISCC-based metadata record. This combination of content-derived identifiers and identity-bound credentials is the basis for a verifiable rights information infrastructure that supports both integrity and provenance tracking in a distributed environment where declarations may be submitted by diverse actors across domains, including cultural institutions, platforms, and (potentially) individual creators.

Liccium provides the software application for Data Suppliers and credential issuers to manage, issue and receive Verifiable Credentials, enabling the secure identification of the party responsible for a content claim.

3.2 Process flows

The CommonsDB system will be structured around three primary interacting parties: Data Suppliers, Third Parties, and End Users, supported by core infrastructure managed by Liccium and CommonsDB consortium members. The registry will operate through two main processes: the declaration of rights information and the search/verification of this information.

3.2.1 Declaration of rights information by Data Suppliers

Data Suppliers (CommonsDB partners who contribute rights information) will make declarations regarding public domain and openly licensed digital assets into the registry. Each declaration includes the following three elements:

1. **Content-Derived Identifier (ISCC):** Data Suppliers will generate ISCC codes locally within their technical infrastructure to create unique identifiers deterministically derived directly from their digital content.

2. **Rights Metadata:** Data Suppliers will provide rights metadata containing information about public domain and openly licensed digital assets, including a registry-supported rights statement (as detailed in section 2.2), and a location URL that provides a reference for the declared work. Data Suppliers can also include other useful metadata about the digital assets in their declarations, such as titles, descriptions, attributions and publication dates.

3. **Verifiable Credentials:** Data Suppliers will supply verifiable credentials with their declarations, ensuring data integrity and proper attribution. To ensure the quality and integrity of the records, proper authentication of the source for each declaration is an important aspect. This is achieved by including publicly accessible verifiable credentials in the metadata records.

The Ingestion Engine, a backend component of the core infrastructure developed by Liccium, will process and integrate declaration metadata from Data Suppliers in the system.

CommonsDB distinguishes between two key components of its content declaration system: Metadata Storage and the Registry. Both are integral to the system's operation but serve distinct purposes and technical roles. The Metadata Storage component is the authoritative, canonical hub for full metadata records. It is used to ingest and store all signed content declarations. Registries are public, use-case specific access points that provide a minimal subset of metadata derived from the full record in storage.

In contrast to the Metadata Storage, the Registry is designed for automatic and highly scalable retrieval and access by machines or platforms. It provides sufficient information to identify the digital assets and derive the legal status from the declaration data set with minimal impact on the technical infrastructure.

The use of verifiable timestamps from third-party time-stamping authorities will ensure the accuracy and validity of content declarations, which will also be digitally signed to enhance authenticity and credibility, with signatures coming with verifiable credentials authenticating content partners and facilitating proper attribution of digital assets.

3.2.2 Search and verification of rights information by Third Parties and End Users

The CommonsDB system will allow both Third Parties (such as repositories, UGC platforms and other types of data aggregators and individual End Users) to search for and verify rights information associated with digital content. This functionality relies on the ISCC as a lookup-key, which allows content partners or other third parties to search, discover, and verify records containing the copyright status of digital assets. From the user's perspective, checking the copyright status of digital assets will be as simple as creating the ISCC and querying the CommonsDB Registry.

Third Parties will be able to search and verify the rights status of digital content at scale by generating ISCC codes locally, implementing a local node of the CommonsDB registry, and searching for exact or similar ISCC codes using a vector search (nearest neighbor search). The CommonsDB Registry is based on peer-to-peer technology that facilitates local synchronization of nodes, containing declarations, ensuring data consistency across the federated network.

End Users will be able to access CommonsDB through a Public User Interface. By uploading a media file, the system will be able to generate its ISCC and retrieve any matching rights information stored in the registry.

The vector search allows searching for the same or similar ISCC code. The Search Engine (provided by Liccium) will enhance this search by enabling efficient querying of the indexed data, such as declaring party or rights status, by End Users and other Third Parties.

4

Analysis of the legal status

This section aims to clarify the legal status of the CommonsDB infrastructure, its key participants, and the relationships among them under EU copyright law. The analysis builds on the technical overview provided in the previous section, referring to the infrastructure elements for a technical and functional explanation of CommonsDB and its workflows. However, the purpose of this analysis is not to provide guidance for assessing the legal status of public domain or openly licensed digital assets whose rights information metadata will be made available via the CommonsDB infrastructure.

4.1 Legal background

CommonsDB functions as a metadata management platform. As outlined in the previous section, it consists of six core components: the Ingestion Engine, the Metadata Storage, the Registry of public domain and openly licensed digital assets, the Public User Interface, the Search Engine, and three APIs (Declaration API, Metadata API, and Search API).

The CommonsDB infrastructure does not host any digital assets to which the metadata relates. In other words, it does not store copyright-protected content – such as works licensed under open licenses – nor does it store content whose copyright protection has lapsed and is now in the public domain. Instead, CommonsDB receives ISCCs, rights metadata, and Verifiable Credentials via the Declaration API from Data Suppliers.

To determine the legal status of CommonsDB, it is necessary to examine its operation within the framework of EU copyright law and platform regulation, particularly concerning copyright and related liability issues. This section,

therefore, provides a basic understanding of relevant EU copyright law and the concepts of primary and secondary liability as they pertain to the question of whether online providers – like CommonsDB – can be held liable for copyright infringement. **Our main conclusion is that in the normal operation of its services, CommonsDB presents no material risk of copyright infringement. We explore certain edge cases and hypothetical scenarios where liability might arise in the interaction between CommonsDB and third parties, which are useful for determining future requirements for an ideal design of the service.**

4.1.1 EU copyright law and primary vs secondary liability

EU copyright law has undergone a high degree of harmonization through numerous directives on copyright and related rights. The interpretation of these directives is shaped by the case law of the Court of Justice of the European Union (CJEU). For our purposes, the most relevant legal instruments are the 2001 InfoSoc Directive, the 2000 e-Commerce Directive (ECD) – now partly amended and replaced by the Digital Services Act (DSA) – and the CDSM Directive.[1]

The term primary liability, used here as a synonym for direct liability, refers to the legal consequence of violating or infringing statutorily defined exclusive rights (e.g., the rights of reproduction or communication to the public) as a primary wrongdoer[2]. Traditionally, direct liability for copyright infringement has been strict.[3] However, the CJEU's interpretation of EU copyright law has arguably modified this traditional approach, particularly concerning acts covered by the right of communication to the public in the online environment. We reference this case law below as we examine CommonsDB.

By contrast, secondary liability applies when the scope of copyright protection is extended – often through national tort laws – to encompass the activities of parties who are not the primary infringers but have contributed to an infringement.[4] This concept covers situations in which an entity facilitates another party's copyright infringement.[5] Secondary liability typically requires both a mental element and a conduct element. The mental element involves assessing the defendant's intent, negligence, or knowledge, which may be general or specific, actual or constructive.[6] The conduct element entails an assessment of whether a provider has complied with reasonable or proportional duties of care to prevent direct infringements.[7] **Although CommonsDB poses no material risks of liability for copyright infringement, it is instructive to examine primary and secondary liability scenarios to identify elements that may inform the optimal design of CommonsDB services and their relationship to third parties.**

4.1.2 Primary liability for copyright infringement: exclusive rights, exceptions and rights management information

EU copyright law has significantly harmonized exclusive rights, exceptions, and, consequently, the framework for primary (direct) liability for copyright infringement. The InfoSoc Directive recognizes exclusive rights applicable to online use, namely reproduction (Article 2) and communication to the public (Article 3), as well as several exceptions and limitations to these rights (Article 5).

Article 2 establishes a broad reproduction right for authors and related rights holders, including performers, phonogram producers, film producers, and broadcasting organizations. Performers and broadcasters also have a specific right of first fixation, meaning the general reproduction right applies only to reproductions of those fixations. Article 3 grants authors a broad right of communication to the public, including the right of making available, while granting related rights holders a narrower right of making available. Article 5 provides the primary legal framework for exceptions and limitations at the EU level. For the purposes of CommonsDB activities, none of the exceptions in this provision are relevant.[8]

In addition to exclusive rights and exceptions, the InfoSoc Directive also regulates technological protection measures (TPMs) and rights management information (RMI) in Articles 6 and 7. This is important because CommonsDB primarily hosts and manages metadata, which could be considered a type of RMI.

RMI refers to information provided by rightholders that identifies a protected work or subject matter, including details about the author, other rights holders, terms and conditions of use, and any related identification numbers or codes. This definition applies when such information is linked to a copy of the content or appears in connection with its public communication.[9] Under the InfoSoc Directive, Member States must provide legal protection against anyone who knowingly and without authorization: Removes or alters electronic RMI; or makes available to the public any protected work or subject matter from which RMI has been removed or altered without authorization. This applies if the person knows or has reason to believe that their actions encourage, enable, facilitate, or conceal copyright infringement.[10] The CommonsDB infrastructure, as we will detail, could enhance the protection of RMI by making its removal more difficult.

4.1.3 Secondary liability and type of service provider

Secondary or "accessory" liability is not harmonized in EU law and is primarily governed by national laws. This makes it difficult to establish clear, common, and consistent rules for online service providers across different Member States.[11] Certain liability exemptions, or "safe harbors," for intermediary service providers were introduced in the ECD and have largely been retained in the DSA.[12] These include a liability exemption for hosting service providers and, by extension, online platforms, which is the focus of our analysis.

Moreover, some scholars categorize specific regimes of intermediary injunctions (e.g., in Article 8(3) of the InfoSoc Directive) as a distinct "third pillar" of liability. This operates in parallel with existing liability rules and helps shape the overall liability framework for intermediary service providers.[13]

Building on this foundation, the DSA introduces a novel regulatory approach by imposing not only liability rules for user-generated content but also separate due diligence obligations regarding how intermediaries design and operate their services. The DSA differentiates between: Rules on the liability of intermediary service providers (Chapter II), and Due diligence obligations for a transparent and safe online environment (Chapter III). [14]

The liability exemptions distinguish between different types of intermediary services, namely "mere conduit," "caching," and "hosting."[15] This framework is largely based on the ECD, with some additions, such as rules on voluntary own-initiative investigations and legal compliance.[16]

Separately, the DSA introduces horizontal due diligence obligations for ensuring a transparent and safe online environment, which were not present in the ECD. These obligations apply asymmetrically to different categories of information society service providers: 1) Intermediary services, 2) Hosting services, 3) Online platforms, and 4) Very large online platforms (VLOPs) and very large search engines (VLOSEs).[17]

The due diligence obligations are cumulative, meaning that as providers move up the scale, they are subject to increasing regulatory requirements. Intermediary service providers have the fewest obligations, while VLOPs and VLOSEs face the most stringent rules. These obligations impose extensive due process, risk assessment, and mitigation requirements. They also cover algorithmic moderation systems and their impact on users' fundamental rights.

To determine how CommonsDB fits within this regulatory framework, it is important to examine the relevant service provider definitions in the DSA:

- **Hosting services** refer to providers that store information on behalf of users.
- **Online platforms** are defined as hosting services that, upon user request, store and disseminate information to the public – unless such activity is only a minor or ancillary feature of another service.[18] These platforms typically include user-uploaded or user-generated content services, such as YouTube, Facebook, or Instagram. As such, the concept of online platform encompasses that of online content-sharing service providers (OCSSPs) under Articles 2(6) and 17 of the CDSM Directive, adding further regulatory complexity.[19]
- **Online search engines** are intermediary services that allow users to search for information across websites based on a query (e.g., a keyword, voice request, or phrase) and return results in various formats.[20]

Based on **CommonsDB's infrastructure and functionality**, we reach the following **preliminary conclusions regarding its classification under the DSA**:

- **Hosting Service Provider:** The Metadata Storage component of CommonsDB qualifies it as a hosting service provider under the DSA.
- **Online Platform:**
  - CommonsDB allows Data Suppliers to submit data (including declaration metadata and content-related information) via the Declaration API and Ingestion Engine for Metadata Storage, which is then made publicly accessible through the CommonsDB Registry.
  - This could qualify CommonsDB as an "online platform" under the DSA, provided that Data Suppliers, Third Parties, and End Users are considered "recipients of the service" – a classification that appears plausible.[21] Doubts remain as to whether the activities of CommonsDB qualify as a "dissemination to the public" under Article 3(k) DSA.
  - If the classification as "online platform" is accepted, CommonsDB would be subject to the DSA's liability exemption for hosting services, and its due diligence obligations applicable to online platforms. If not, the CommonsDB need only comply with the obligations applicable to hosting service providers.

- Importantly, however, CommonsDB does not host copyright-protected content. As such, it does not qualify as an OCSSP under the CDSM Directive.

- **Online Search Engine:**

  - Liccium's search engine, which is accessible through the Public User Interface, likely does not qualify as an "online search engine" under the DSA, since it does not enable "searches of, in principle, all websites, or all websites in a particular language" (Art. 3(j) DSA). As such, CommonsDB does not benefit on this account from the liability exemption for either hosting services or mere conduit services (depending on whether the exemption extends to search engines), and is also not subject to the obligations specific to online search engines (mainly related to transparency requirements under Chapter III of the DSA).

In sum, CommonsDB may be classified under the DSA as a hosting service provider, and possibly an online platform, depending on how its users and functionalities are interpreted. If these classifications apply, CommonsDB would benefit from the hosting liability exemption and be subject to specific due diligence and transparency obligations under the DSA. From a holistic perspective, we propose that the most adequate characterization of CommonsDB is as a metadata platform, which comprises hosting and search functions.

4.2 Legal analysis of CommonsDB

This section assesses the legal status of the infrastructure hosted by CommonsDB, a metadata platform. This section explores scenarios where liability under copyright law could theoretically arise and considers that the use of digital assets by an upstream Data Supplier may be governed by an open license, rather than the expiration of copyright protection. The analysis demonstrates that any potential liability is limited to edge cases occurring under very specific and narrow circumstances. Although the identified risks remain minimal and contingent (i.e., reliance risks), understanding potential avenues for liability is valuable, as it helps inform and structure relationships with Data Suppliers and other third parties. Accordingly, the analysis in the following sections serves not only to clarify the legal status but also to guide how prudent interactions within the existing legal framework can be shaped within the CommonsDB infrastructure. Importantly, as our analysis clarifies, the normal operation of CommonsDB gives rise to no material liability risks from a copyright perspective.

CommonsDB comprises six core components: the Ingestion Engine, the Metadata Storage, the Registry of public domain and openly licensed digital assets, the Public User Interface, the Search Engine, and three APIs (Declaration API, Metadata API, and Search API). Using these components as a reference framework, the section is divided into four subsections:

- The copyright status of digital assets (4.2.1);
- Copyright-relevant uses occurring internally within the CommonsDB infrastructure (4.2.2);
- Copyright-relevant uses resulting from the provision of services to third parties (4.2.3); and
- A risk exposure assessment (4.2.4).

4.2.1 Public domain status of digital assets

The legal risk and exposure for CommonsDB depend on how the public domain and openly licensed status of digital assets have been established. It is useful to distinguish between two categories:

1. Digital assets whose copyright has lapsed (public domain proper);
2. Digital assets made available through rights waivers or open licenses (currently: CC0, Public Domain Mark, CC BY, CC BY-SA).

In the first case, no copyright issues appear to arise, as protection has lapsed by law. In Europe, this typically applies to works whose authors died before 1954, given the 70-year post mortem auctoris (p.m.a.) term set by the Term Directive.[22] [23] For neighboring rights (e.g., performances, recordings, broadcasts), the term varies depending on whether the work was published and its type – generally 50 or 70 years from fixation or publication.[24] [25]

However, Article 4 of the Term Directive is key for cultural heritage: it grants 25 years of protection to previously unpublished works once they are lawfully made public, even if original copyright has expired. Thus, private recordings or photos may still be protected if only recently disclosed. Finally, some Member States, like France and Poland, provide indefinite moral rights protection, requiring proper attribution of authorship.

For the second category of digital assets, no such presumption can be made, as their public availability status relies on a license or rights waiver. This necessitates a copyright compliance analysis in cases where a rightsholder attempts to revoke the license or where defects waiver or license exist – such as the rightsholder's inability to waive certain rights, or where the Data Supplier's use falls outside the scope of the waiver or license. Broad rights waivers and licenses, such as CC0 or CC BY, are designed with these legal complexities in mind, aiming to enable the widest possible use within the limits of national law.[26]

4.2.2 Copyright-relevant use within the CommonsDB infrastructure (storage)

With the CommonsDB infrastructure and the public domain status of digital assets in mind, the fundamental question is whether CommonsDB performs any copyright-relevant acts internally within its infrastructure. **It is clear from the nature of the infrastructure that no acts of reproduction take place.**

As a metadata platform, CommonsDB does not host any of the Digital Assets to which the metadata refers. Instead, it receives ISCCs, Rights Metadata, and Verifiable Credentials via the Declaration API from Data Suppliers. None of the data operations within the CommonsDB infrastructure – whether through the Declaration API, Metadata Storage, or retrieval of information following a database search – involve copies of works. Rather, they concern only declaration metadata and content-related information obtained from Data Suppliers.[27]

It can therefore be stated with certainty that CommonsDB does not carry out any reproduction of digital assets within the meaning of Article 2 of the InfoSoc Directive, nor is its infrastructure used by others to perform a restricted reproduction.

Since ISCC generation occurs locally on the Data Suppliers' servers,[28] any temporary reproductions made during the analysis of a digital asset – solely for the purpose of generating an ISCC and retrieving relevant metadata – are confined to the Data Supplier's infrastructure before being transmitted to the CommonsDB Ingestion Engine.

4.2.3 Copyright-relevant use resulting from provision of service

The operation of CommonsDB raises additional copyright considerations because interactions and exchanges of information with Data Suppliers, Third Parties, and

End Users require the CommonsDB infrastructure to be accessible to these parties. **In the normal course of operation and for the vast majority of cases such a feature will generally not raise copyright concerns, precisely because CommonsDB does not host any copies of protected material.** However, such concerns may be raised in the special case that digital assets, whose metadata CommonsDB processes, are used by the Data Supplier without authorization when those turn out to not be in the public domain or are alternatively used in breach of specific terms attached to the use of the asset. As copyright infringement generally is a strict liability offense, even the most unpredictable of situations will have copyright significance despite that a Data Supplier may diligently follow the terms of an open license; for example when copyright co-authorship is established after several decades and the new co-author objects to the open license.[29] The present section therefore surveys the legal framework to assess the status of CommonsDB by accounting for the outcome that a relevant Third Party may, for whatever reason, be itself exposed to copyright liability.

4.2.3.1 Protection of Rights Management Information, moral rights and conflict resolution

Rights Management Information (RMI)

CommonsDB is a metadata platform that will be used to host and make RMI available. Its setup will contribute to better protection of RMI by making its removal more difficult.

As factual information, metadata does not fall under proprietary copyright protection. Therefore, its processing and storage – once received from Data Suppliers – do not implicate as such the right of reproduction or any other exclusive right. However, as noted, Article 7 of the InfoSoc Directive protects RMI from removal or alteration. RMI includes “any information provided by rightholders which identifies the work or other subject matter (...), or any other rightholder, or information about the terms and conditions of use of the work or other subject-matter, and any numbers or codes that represent such information.”

Accordingly, metadata that identifies the author or rightholder, or that describes terms and conditions of use, and is ingested into CommonsDB following ISCC generation, qualifies as RMI under Article 7. The ISCC itself likely does not fall within this definition, as it identifies a work, but not the author or usage terms. Thus, even if copyright metadata is not protected as proprietary content, it is still necessary to observe the liability provisions regarding the protection of RMI.

CommonsDB is not designed to alter information submitted by Data Suppliers – nor does it, on its own initiative, remove or alter such information, including that received from Third Parties synchronizing their repositories with the CommonsDB registry. As such, CommonsDB would not breach Article 7. Any unlawful removal or alteration of RMI, or communication of works from which RMI has been removed or altered without authority, would require that CommonsDB had knowledge or reasonable grounds to know that such actions would induce, enable, facilitate, or conceal copyright infringement (Article 7(1) InfoSoc Directive). In other words, CommonsDB would need to act intentionally or negligently in altering or removing copyright-relevant information. This is clearly not the case.

As a neutral and passive intermediary between Data Suppliers, Third Parties, and End Users, CommonsDB operates as a metadata registry and repository, relaying information received from trusted external sources. For CommonsDB to have reasonable grounds to suspect an infringement, there would need to be clear indications that a Data Supplier or Third Party consistently submits erroneous or misleading information in bad faith. With that said, it is important to emphasize that CommonsDB is designed to attach RMI (such as licenses and the public domain status of digital assets) directly to the assets themselves. This not only makes it easier for third parties to access RMI in order to obtain or verify copyright information but also ensures that such data is preserved. In other words, CommonsDB serves as a technical solution to the problem that Article 7 of the InfoSoc Directive seeks to address through legal prohibition.

Moral Rights

Beyond RMI, the protection of moral rights is also relevant to CommonsDB's operations. Moral rights are not harmonized at the EU level[30], but they are recognized under Article 6bis(1) of the Berne Convention and Article 1(4) of the WIPO Copyright Treaty (WCT), which incorporates the Berne provision. While Article 6bis(2) requires protection of moral rights for at least as long as economic rights, several Member States provide indefinite protection, reflecting the personal connection of the author to their work.[31]

Of particular importance is the right to claim authorship, which from a copyright perspective is a key piece of metadata that may be processed by the CommonsDB infrastructure. In particular, the envisaged design of CommonsDB is that Data Suppliers have the option of providing information about authorship in addition to other mandatory information.[32] As a result, the CommonsDB registry can assist with moral rights compliance online whenever Data Suppliers avail themselves of the opportunity to provide authorship information.

Nevertheless, like infringement of economic rights, infringement of moral rights generally does not require intent or negligence.[33] Therefore, if erroneous authorship information is present in the registry and can be linked to a particular work (data asset), CommonsDB could in theory be exposed to liability – even if the error originates from a Data Supplier. However, the risk is reduced when Third Parties consult the CommonsDB Registry for data synchronization purposes, as conflicting entries may highlight discrepancies. Ultimately, however, because CommonsDB enables the binding of copyright information to digital assets, it can contribute to genuine moral rights compliance in the digital environment.

Conflict resolution

Closely tied to the protection of RMI and moral rights is conflict resolution, particularly in cases involving identical or similar ISCCs associated with differing metadata, Data Suppliers, or timestamps. Such conflicts may indicate the presence of erroneous information in the registry. Resolving these conflicts further lowers the already low risk of violation of moral rights and RMI protection – especially when copyright-relevant metadata is involved.

Although CommonsDB has access to metadata and can analyze the nature of a conflict, it operates – from a legal perspective – as a neutral and passive information provider. However, CommonsDB does not undertake any proactive search, verification, or manual comparison of metadata entries. Therefore, at this stage an envisageable approach to resolving conflicts is to tether information to the Data Supplier that submitted the original information, letting that party rectify potentially incorrect data. In other words, CommonsDB would not act beyond intermediating information.

4.2.3.2 Communication to the public

The exclusive right of communication to the public was briefly explained above.

For the most part, this right is irrelevant in this context. Since CommonsDB does not host digital assets, it does not operate on them and therefore cannot make or transmit those assets to the public. In this respect, CommonsDB is not communicating or making works available to the public in any of the typical scenarios usually relevant for copyright purposes, such as via a platform's own infrastructure [34], a web page, or a hosting service.[35]

However, expansive interpretations of Article 3 – particularly by the CJEU – have extended direct liability to cases involving facilitation of infringement. Of note is the C-610/15 – Ziggo case, concerning The Pirate Bay. The CJEU held that the right

of communication to the public encompasses the operation of a sharing platform which, through indexation of metadata and a search engine, allows users to locate and share infringing content via a peer-to-peer network – provided the operators have full knowledge of the consequences of their conduct.[36]

These types of uses may be described as secondary communications to the public, where the intermediary does not host content directly but enables or facilitates access to protected content.[37] Under this framing, certain components of the CommonsDB infrastructure – primarily designed to provide access to stored metadata – could warrant an assessment of the legal status of CommonsDB:

- The **Search API** and **Public User Interface**, which allow End Users and Third Parties to interact with the system and query indexed data;
- The **Metadata API**, which enables Third Parties to access stored metadata for third-party integration purposes;
- The ability to **synchronize Third Party registries** with the CommonsDB Registry containing declaration metadata from Data Suppliers.

At this stage, **it is important to clarify that, as a good-faith metadata platform, CommonsDB occupies a completely different legal position than services designed to facilitate access to unlawful content. The *Ziggo* judgment is therefore useful primarily for understanding the boundaries of liability for communication to the public under EU copyright law and, in our view, for informing the optimal design of an online service that interacts with third-party suppliers of copyright-related data.**

With this framing in mind, the following factors are important when assessing liability under the ***Ziggo* judgment and may be useful to inform how CommonsDB designs its interaction with third parties**.

- **Communication to the public:** The communication must be directed to an "indeterminate number of potential recipients," implying a fairly large group.[38] If CommonsDB restricts access to defined categories of End Users or Third Parties, then it is arguable that its operation is not directed to the public as required under Article 3.[39] However, since the Public User Interface is accessible to internet users, the application of Ziggo cannot be dismissed outright, at least for that part of the service.

- **Findability of the original resource:** The metadata accessible via CommonsDB must lead to the original source, i.e. the Data Supplier hosting the digital asset. In normal operations, such as when an End User conducts a content search, the metadata includes a resource URL provided by the Data Supplier, indicating where the asset is hosted. If no such URL is present, the asset is not findable through CommonsDB, eliminating potential liability under Ziggo.

- **Infringing nature of the asset:** For liability to arise, the asset must be infringing – for example, used without authorization or outside the bounds of a valid copyright exception. Alternatively, it may be used in breach of license terms (e.g., published online without watermark protection when a license required it). Liability under Ziggo hinges on such infringement, along with the presence of a deliberate intervention by the intermediary that enables access.[40] This is a particularly **unlikely scenario for CommonsDB** since the assets in question are either in the **public domain or subject to open licenses**, and **hosted by good faith, diligent third parties**. Furthermore, CommonsDB is a good faith provider that in no way intervenes to facilitate copyright infringement. As a result, **it is difficult to envisage a situation where CommonsDB is subject to direct liability under *Ziggo***.

- **Knowledge of infringement:** The final, and perhaps most ambiguous, factor is whether the operator had full knowledge of the consequences of their conduct.[41] In Ziggo, it is unclear whether the CJEU required knowledge of the infringing nature of the content or simply awareness that the platform facilitates access to such content. While the Court acknowledged the illegality of the content in its assessment, it did not clearly state that this was a necessary condition for liability. Our reading of the CJEU case law in this area is that knowledge of the infringing nature of the content is a prerequisite for liability under Ziggo.[42]

In conclusion, CommonsDB does not assess the copyright status of digital assets hosted elsewhere. Nor is it in a position to determine whether a Data Supplier has acted outside the scope of a license, misrepresented a public domain status, or acted in bad faith when submitting data. Therefore, ***Ziggo*-type** liability for providing access to indexed metadata – whether through the Public User Interface, Metadata API, or Registry synchronization – is **unlikely**.

An hypothetical scenario that is worth considering is that where CommonsDB is made aware that metadata in the CommonsDB Registry contains erroneous information about the public domain or copyright status of a digital asset, implying potential infringement (economic or moral) by the Data Supplier.

In such cases, safe harbor provisions, particularly Article 6 of the DSA (formerly Article 14 ECD), may apply. If CommonsDB is considered a hosting provider of what would in such a hypothetical scenario be considered as illegal information (metadata) uploaded by Data Suppliers and Third Parties, Article 6 DSA could shield CommonsDB from liability – provided it acts expeditiously upon receiving notice of infringing content to remove or disable access to the problematic metadata information. But even this scenario requires first a determination that the metadata in question is illegal because it constitutes copyright infringement, which is far from clear. In our view, any issues arising from this scenario are sufficiently addressed by CommonsDB conflict resolution mechanisms identified above.

4.2.3.3 Secondary liability issues

As mentioned in the introduction, secondary liability is a matter governed by national copyright law. It presupposes that an infringement has occurred, which – given the technical process flow – would, in this context, involve activities undertaken upstream by Data Suppliers.

Importantly, even if expansive interpretations of Article 3 of the InfoSoc Directive by the CJEU have elevated certain acts of facilitation of infringement to primary liability under harmonized EU copyright law, thus shifting the issue away from national discretion, there may still be reasons to account for national secondary liability doctrines.

A significant example is secondary liability in Sweden. In 2017, in the B2 Bredband case, the Swedish Patent and Market Court of Appeal (PMÖD) introduced a civil law definition of contributory copyright infringement, effectively broadening the concept to include what appears to be the mere provision of a service.[43]

This case concerned the issuance of a website-blocking injunction against a good-faith ISP. It has since been successfully applied in nearly all subsequent website-blocking injunction cases in Sweden, consistently resulting in ISPs being found liable for contributory infringement merely for providing internet connectivity to their customers – even though the infringing activity is actually committed by third-party resources on the open internet.[44] In theory, considering the breadth of the definition, the same standard could apply to other types of intermediaries in a civil copyright case, such as a hosting provider or a metadata platform that facilitates user access to protected content.

However, that outcome is unlikely here since CommonsDB collaborates with good faith and diligent Data Suppliers that by default host digital assets that are in the

public domain or under open licenses. As a result, also for secondary liability purposes, there appears to be no material risk of infringement.

4.2.4 Risk exposure assessment - copyright issues

Overall, compared to models where information or content is permanently or temporarily uploaded for classification, CommonsDB is designed to operate differently: the infrastructure receives only metadata. Data Suppliers generate ISCCs and related metadata locally, before submitting it to the system. This structure does not entail any risk of direct infringement through reproduction, as CommonsDB never makes or processes a copy of the underlying digital material. This design also reduces reliance-based risks, meaning risks that are associated with trusting or depending on data and information submitted by third parties (e.g. a Data Supplier) – and that this reliance could lead to negative consequences if that source fails or proves to be unreliable. Although CommonsDB cannot independently verify such information, it works only with trusted Data Suppliers. In doing so CommonsDB minimizes any reliance risks associated with improper license attribution to digital assets.

The theoretical risk in this scenario is that if incorrect metadata is provided by a Data Supplier – whether by error or misrepresentation – that erroneous information propagates through the system, potentially misleadingThird Parties regarding the copyright status of a work. This role as an information provider could in edge cases expose CommonsDB to liability, either through reliance-based claims or, depending on the jurisdiction, contributory liability when a Data Supplier infringes copyright.

While CommonsDB is designed to function with partners acting in good faith, it is important to underscore that even if incorrect information is processed, liability arises under copyright law, not from any contractual arrangement. The terms of a waiver or license are enforceable only against the Data Supplier, not against CommonsDB, since CommonsDB does not host the content and is therefore not a licensee or beneficiary under any such arrangement. Moreover, under the principle of privity of contract, CommonsDB (as a third party) is generally not bound by the terms of a license or waiver. Any potential liability would therefore arise from the proprietary nature of copyright, with its erga omnes effect, not from a contractual obligation.

Accordingly, CommonsDB's copyright compliance obligations are rooted in the legal framework, not in any upstream contractual arrangements. However, if CommonsDB were to to publish records or information that incorrectly identifies

digital assets as being in the public domain, a circumstance that can only occur if the data submitted by the Data Supplier is incorrect, the key legal issue becomes whether the indexing of (incorrect) metadata and the offering of search functionality amounts to a "making available" of works to the public, as interpreted by the CJEU in *C-610/15 – Ziggo*, examined above.

But as outlined above, for ***Ziggo*-type** liability to apply, CommonsDB would need to have full knowledge of the erroneous public domain status of the work, or of non-compliance with licensing terms by the Data Supplier. Liability would only arise if CommonsDB, upon being notified, were unwilling to take corrective action, particularly by removing the resource URL linking to the infringing digital asset, e.g. under its conflict resolution rules. Overall, we view this as a very unlikely scenario.

Additionally, in certain jurisdictions, CommonsDB could be subject to broad secondary liability regimes, where even passive service provision, such as enabling access to content hosted elsewhere, may suffice to establish liability. The extent to which this applies is a matter of national law, and the bona fide character of CommonsDB's and Data Supplier's operations would either eliminate or mitigate liability in such cases.

4.3 Data governance issues

Data governance plays a vital role in the current EU regulatory landscape, despite its relatively recent emergence. Its prominence reflects the European Commission's broader policy goal of unlocking the value of data within the fragmented EU internal market – essential for enhancing global competitiveness.[45]

Key legislative initiatives in this area – referred to here as data legislation – include the Data Governance Act (DGA) and the Data Act (DA), which are the focus of this analysis. However, related instruments such as the Digital Markets Act (DMA), DSA, AI Act, and European Health Data Space Regulation (EHDSR) form part of the same overarching policy. [46] Only by viewing these measures collectively can the full impact of this new regulatory framework be understood.

Under EU law, "data" is broadly defined as any digital representation of acts, facts, or information – including sound, visual, or audiovisual recordings.[47] This definition can overlap with subject matter protected by copyright or related rights. As a result, data may also qualify as works or other protected content under the EU copyright framework.[48]

A key feature of data legislation is its reliance on public law concepts, such as "data access" and "data portability", rather than traditional private law (including IP law). The creation of regulatory bodies with oversight roles also reflects this shift. This regulatory approach poses challenges when aligning conventional copyright assessments with new legal obligations that may concern the same or related data.

4.3.1 The Data Act and CommonsDB

The Data Act (DA) addresses specific types of data to correct market failures in the EU's data economy, particularly where data is concentrated in the hands of large companies or locked in by certain market structures or technologies.

Our analysis concludes that most of the obligations in the DA do not apply to CommonsDB. There are however certain provisions that may be relevant in this context, namely in Chapters IV (Provisions on data contracts) and VI (Switching between data processing services) and VIII (Interoperability requirements).

Chapter IV on data contracts may be relevant. If data is contributed by third parties or suppliers via formal agreements, these could qualify as data contracts. This chapter regulates terms on data access, use, liability, and breach/ termination. It applies only when a contractual term is unilaterally imposed and deemed unfair, respecting overall contractual freedom. The application of this chapter presupposes business activity. Chapter IV applies to contracts between enterprises. The concept of "enterprise", specified in Art. 2.24 DA, includes any entity acting in a professional or economic capacity, regardless of profit orientation. Thus, organizations like those operating CommonsDB may still fall within scope if they engage in economic activities. Notably, Art. 9(4) explicitly references data recipients who are SMEs or not-for-profit research organizations, reinforcing this possibility. A tailored analysis is needed to determine whether CommonsDB's structure, funding, or activities trigger obligations under this chapter.

Chapter VI governs switching between data processing services (DPS), defined as services offering on-demand access to configurable, scalable computing resources (Art. 2.8). Whether CommonsDB – or specific components like its Ingestion Engine, Metadata Storage, or Search API – qualifies as a DPS requires further analysis. The chapter's aim is to enhance data portability and reduce vendor lock-in. Given CommonsDB's open standards and transparent design, it likely aligns in principle – if not yet fully in technical terms – with these goals. However, compliance with provisions on technical, organizational, contractual,

and commercial switching barriers should be assessed. Art. 31.2 also exempts services used for testing and evaluation.

Chapter VIII addresses interoperability and standardization, particularly for data spaces, DPS, and smart contracts related to data sharing. Its relevance to CommonsDB depends on whether the project qualifies as a "data space" – defined as a framework for sharing or jointly processing data for research, innovation, or civil society purposes (Rec. 103). Regardless, CommonsDB's reliance on public standards and transparency likely supports or even fulfills these interoperability aims. Still, this chapter warrants closer review.

4.3.2 The Data Governance Act and CommonsDB

The DGA outlines four main frameworks for voluntary data sharing, each potentially relevant to CommonsDB:

- Chapter II – Data held by public sector bodies but protected by third-party rights (outside the scope of the Open Data Directive, or ODD);
- Chapter III – Data intermediaries facilitating sharing between data holders/subjects and users;
- Chapter IV – Data altruism, i.e., voluntary, non-remunerated data sharing for general interest purposes;
- Establishment of the European Data Innovation Board (EDIB), supporting the EU Data Strategy, standardization, and Common European Data Spaces (European Commission, 2024).

Regarding Chapter II, it is noted that the ODD promotes re-use of public sector data but excludes data protected by copyright or containing personal data. The DGA complements the ODD by enabling re-use of such protected data under specific conditions – e.g., access to anonymized data or use within secure environments. Where re-use isn't possible, public bodies must support users in obtaining the necessary consent (Baloup et al., 2021).

Applicability to CommonsDB depends on whether the metadata platform, Data Suppliers, or Third Parties qualify as public sector bodies under the ODD/DGA, and whether the data is protected. Basic works metadata (author, year, title) is likely factual and unprotected. While complex metadata could, in rare cases, meet the originality threshold for copyright, this seems unlikely, as noted in our

previous analysis. Potential proprietary claims may arise if the metadata set qualifies for the sui generis database right or if the database structure is original. However, as Data Suppliers – who are likely the rights holders – voluntarily provide metadata, standard contracts can likely address rights and permissions. CommonsDB, for its part, makes no proprietary claim or imposes any access restriction on the metadata in its infrastructure.

Chapter III introduces a framework for data intermediation service providers, defined as services establishing commercial relationships for data sharing between data subjects/holders and users. These include data-sharing ecosystems and markets. Given CommonsDB's non-commercial, open-access mission, it likely does not qualify as an intermediation service. Recital 29 confirms that repositories supporting open-access scientific data re-use are excluded from this category. However, if CommonsDB's structure or activities evolve, this classification may need revisiting. Intermediaries face strict obligations: they may not use data for other purposes, must separate intermediation from application services, and must act in users' best interests (e.g., informing data subjects of uses and conditions).

The DGA in Chapter IV also defines Data Altruism Organizations (DAOs) – entities facilitating voluntary data sharing without reward (except cost recovery) – for purposes like scientific research. This concept may be relevant to CommonsDB, especially for Data Suppliers and Third Parties. As with data intermediaries, there are concerns for DAOs about the burden of compliance and limited incentives to register through the framework. Ongoing developments include the Rulebook for DAOs (Art. 22) and a standardized European Data Altruism Consent Form (Art. 25), both pending adoptions.

5

Open issues

As stated in the introduction, the primary purpose of this first part of the feasibility study was to make our development approach and design choices transparent to enable stakeholder feedback.

Our subsequent report will explore a number of additional legal and operational questions that we have not addressed in this study. Such questions include the authorization required from aggregators for registry declarations on behalf of CHIs, and the resolution of conflicting rights statements.

These and other issues will be addressed in the second part of the study, which we plan to publish in November 2025. By that time, we plan to have the core registry infrastructure up and running, so the follow-up part will be informed by the practical issues we expect to encounter in the coming months.

5.1 Operational issues

As outlined in the first three sections of this study, the design and implementation of the CommonsDB is based on a number of assumptions about how technological elements (such as content-derived identifiers, digital signatures, a central registry) can be used to provide greater legal certainty. These assumptions will need to be validated in practice as the prototype is built. At this stage, we can identify two areas that will require careful attention to get the implementation right:

- The first is the trust model built into the system. In the initial phase of the prototype, we are using a relatively simple model in which Open Future issues verified credentials to our data partners (initially these are also project partners, although we will seek to include additional partners in the second half of the project). Given the existing relationships, extending trust to these partners is relatively straightforward. Given the ambition to open

up the system to additional data providers, we will need to develop a trust model for assessing the trustworthiness of data providers, define minimum thresholds and other criteria to ensure the overall reliability of the declarations published through the registry, and develop a better understanding of how to deal with aggregation chains (at what level of such a chain should declarations be made). All of this will need to be reconciled with a technical approach to managing the credentials that underpin the technical trust model embedded in CommonsDB.

- The second is the relationship between digital assets (which we can identify using ISCC codes) and more abstract concepts such as 'work'. This is particularly relevant where individual works are represented by multiple digital assets, such as in the case of composite works, collections or objects that are reproduced in multiple ways. We need to understand how our approach based on per-asset identifiers can be used to express information about such higher-level concepts and how these fits with existing collection management practices of our data providers. This point is likely out of scope for the 2nd part of the feasibility study as we do not expect to have sufficient experience by November.

Finally, we will also need to evaluate how the prototype we are building can be integrated into existing infrastructures. This evaluation should include the rights information services currently provided and explored by the EUIPO and the Common European Data Space for Cultural Heritage.

5.2 Legal issues

There are also a number of legal questions which we will analyze in more detail in the second part of the feasibility study. Based on our existing analysis and understanding of the system, these include three issues:

1. How should CommonsDB deal with conflicting rights information in the system. In other words, what should happen if there are declarations that relate to the same digital asset but indicate different copyright statuses? There are two sub-issues here:

    a. where one of the statements is incorrect (e.g. someone states that a work is in the public domain, and someone else claims it is still in copyright – even though it is clearly not). This is a real conflict.

b where both statements are correct (e.g. an in-copyright work available under two different CC licenses, or a work that is in the public domain in one jurisdiction but not in another).

2 A closer look from the legal perspective at the effect of digitally signing them. What (if any) is the difference in effect, validity, trust, or liability between a digitally signed declaration and more traditional ways of publishing rights information (e.g. as metadata alongside or embedded in a digital asset)?

3 An exploration of how rights statements are determined by our two data partners, with the aim of understanding how their practices affect the trustworthiness of the rights information. This is interesting because our data partners follow two different approaches: a process based on institutional trust (Europeana) and a process based on the wisdom of the crowd (Wikimedia Commons). Both approaches likely produce different levels of trust and accuracy. The outcome of this analysis will help us formulate criteria for determining how CommonsDB can assess the trustworthiness of third-party contributors to the system (see also the second sub-point under operational issues above).

These issues provide us with initial starting points for the second part of the feasibility study which will be delivered in November 2025.

Annex: CommonsDB metadata scheme

The following tables detail the metadata scheme for the CommonsDB registry. The first table specifies which metadata Data Suppliers can include in declarations via the Declaration API, along with the field names, descriptions, storage locations (Metadata Storage and Registry), and whether the fields are required or optional. The second table outlines technical metadata that is intrinsic to the registry, such as metadata about credentials, signatures, and declarations.

Data Supplier metadata

Field	Description	Metadata Storage	Registry	Required?
location	**Reference URL for the page where the work is presented**	**Yes**	**Yes**	**Yes**
rightsStatement	**Machine readable statement indicating the copyright and reuse status of a work**	**Yes**	**Yes**	**Yes**
name	**Title of the work**	**Yes**	**No**	**Yes**
creationDate	**Date on which the work was created**	**Yes**	**No**	**No**
pdRationale	**Rationale for determination that a work is in the public domain**	**Yes**	**No**	**No**
description	**Description of the work**	**Yes**	**No**	**No**
creator	**Creator of the work**	**Yes**	**No**	**No**
cdbTdmOptout	**Information on possible TDM opt-out**	**Yes**	**Yes**	**No**
attributionString	**Attribution string (byline) for using a work**	**Yes**	**No**	**No**
steward	**Name of the person/organisation making the work available, if different from the declaring party**	**Yes**	**No**	**No**

Technical registry metadata

Internal

Field	Description	Metadata Storage	Registry
companyId	**Identifier for a company or organization**	**Yes**	**No**
declarerId	**Identifier for the person or system making the declaration**	**Yes**	**No**
iscc	**Unique identifier for the media asset generated by the ISCC Generator**	**Yes**	**Yes**
declarationId	**Unique identifier for the declaration record**	**Yes**	**Yes**
cid	**Self-describing content-addressing identifier and a cryptographic hash of the metadata**	**Yes**	**Yes**

Signature metadata

Field	Description	Metadata Storage	Registry
signature	**Base64-encoded or hex-encoded digital signature over the declaration data**	**Yes**	**Yes**
tsaSignature	**Timestamp authority signature over a hash or document, typically RFC 3161-compliant**	**Yes**	**Yes**
commonsDb Registry Signature	**Base64-encoded or hex-encoded digital signature over the declaration data**	**Yes**	**Yes**
commonsDb RegistryTsa Signature	**Timestamp authority signature over a hash or document, typically RFC 3161-compliant**	**Yes**	**Yes**

Declaration metadata

Field	Description	Metadata Storage	Registry
iscc	**Unique identifier for the media asset generated by the ISCC Generator**	**Yes**	**Yes**
version	**Version of the declaration or metadata schema**	**Yes**	**No**
entryUUID	**Unique identifier for the entry from an a uthority source, could be a UUID**	**Yes**	**No**
createdAt	**Timestamp when the record was first created**	**Yes**	**No**
updatedAt	**Timestamp of the most recent update**	**Yes**	**No**
timestamp	**General-purpose timestamp of the event**	**Yes**	**Yes**
declarerId	**Identifier for the person or system making the declaration.**	**Yes**	**No**
regId	**Registry identifier**	**Yes**	**No**

declarationId Version	**Version of the declarationID**	**Yes**	**No**
$schema	**URI of the JSON schema used to validate the structure**	**Yes**	**No**
mediatype	**Media type of the declared content (MIME type)**	**Yes**	**No**
thumbnail	**Base64-encoded image embedded as a Data URI, typically a small preview of the original content**	**Yes**	**No**
original	**Indicates whether the declaring party claims to be the original creator or rightsholder of the content**	**Yes**	**No**

Credentials metadata

Field	Description	Metadata Storage	Registry
id	**Unique identifier for the credential**	**Yes**	**No**
type	**Credential types indicating its structure and semantics**	**Yes**	**No**
(proof) type	**Type of cryptographic proof used**	**Yes**	**No**
jwt	**Signature in JWT format**	**Yes**	**Yes**
issuer	**Identifier of the credential issuer, typically a DID**	**Yes**	**No**
validFrom	**Start time when the credential becomes valid**	**Yes**	**No**
validUntil	**Expiration time of the credential**	**Yes**	**No**
pii	**Classification of personal data sensitivity**	**Yes**	**No**
(termsOfUse) type	**Policy type governing use**	**Yes**	**No**
confidentiality Level	**Access level for the credential data**	**Yes**	**No**
(schema) id	**URI to the schema definition**	**Yes**	**No**
type	**Type of schema definition (e.g. JsonSchema)**	**Yes**	**No**
(subject) id	**Identifier of the subject (often a DID)**	**Yes**	**No**
sameAs	**Indicates that the subject is also identified by another URI**	**Yes**	**No**
dataSupplierFor	**Identifies the role of the declaring party**	**Yes**	**No**

Notes

[1] Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information society (Information Society Directive, InfoSoc Directive) [2001] OJ L167 (hereafter InfoSoc Directive); Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (e-Commerce Directive) [2000] OJ L171 (hereafter ECD); Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC (hereafter CDSM Directive); Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (hereafter Digital Services Act or "DSA"). N.B. The ECD and DSA are not strictly part of the EU copyright acquis.

[2] Martin Husovec, 'Remedies First, Liability Second: Or Why We Fail to Agree on Optimal Design of Intermediary Liability?' in Giancarlo Frosio (ed), The Oxford Handbook on Intermediary Liability (OUP 2021)

[3] Christina Angelopoulos, 'Harmonising Intermediary Copyright Liability in the EU: A Summary' in Giancarlo Frosio (ed), The Oxford Handbook of Online Intermediary Liability (Oxford University Press 2020)

[4] Husovec, 'Remedies First, Liability Second' (n 2); Christina Angelopoulos, European Intermediary Liability in Copyright: A Tort-Based Analysis (Kluwer Law International 2016). See also Matthias Leistner, 'Structural Aspects of Secondary (Provider) Liability in Europe' (2014) 9 Journal of Intellectual Property Law & Practice 75.

[5] Some authors, like Angelopoulos, refer to this category in the context of copyright instead as "accessory" liability; others yet, like Leistner, also use the term "contributory" liability Leistner, 'Structural Aspects of Secondary (Provider) Liability in Europe' (n 4).

[6] Angelopoulos and Quintais (n 4); Angelopoulos, European Intermediary Liability in Copyright: A Tort-Based Analysis (n 4).

[7] See, e.g. Leistner, 'Structural Aspects of Secondary (Provider) Liability in Europe' (n 4).

[8] See e.g. João Pedro Quintais, *Copyright in the Age of Online Access: Alternative Compensation Systems in EU Law* (Kluwer Law International 2017); Tito Rendas, *Exceptions in EU Copyright Law: In Search of a Balance Between Flexibility and Legal Certainty* | (Kluwer Law International 2021); Eleonora Rosati, *Copyright and the Court of Justice of the European Union* (Oxford University Press 2019). Recent flexibility can be identified e.g. in the trilogy of Grand Chamber judgements in: Case C-476/17 *Pelham and others*, EU:C:2019:624; Case C-516/17 *Spiegel Online*, EU:C:2019:625; Case C-469/17 *Funke Medien NRW*, EU:C:2019:623.

[9] Article 7(2) InfoSoc Directive

[10] Article 7(1) InfoSoc Directive.

[11] Leistner, 'Structural Aspects of Secondary (Provider) Liability in Europe' (n 4); Angelopoulos, *European Intermediary Liability in Copyright: A Tort-Based Analysis* (n 4); Husovec, 'Remedies First, Liability Second' (n 4).

[12] Chapter II and art. 89 DSA.

[13] The "third pillar" characterization is made by Husovec, 'Remedies First, Liability Second' (n 2).

[14] NB the liability exemption rules and due diligence obligations are separate from each other. That is to say, as a rule the availability of a liability exemption is not dependent on compliance with due diligence obligations and vice-versa.

[15] Articles 4 to 6 DSA.

[16] Articles 7 to 10 DSA.

[17] In the scheme of the DSA hosting providers are a type of provider of intermediary services, online platforms a type of hosting provider, and VLOPs a type of online platform.

[18] Art. 3(i) DSA (with further specificity).

[19] João Pedro Quintais and Sebastian Felix Schwemer, 'The Interplay between the Digital Services Act and Sector Regulation: How Special Is Copyright?' (2022) 13 European Journal of Risk Regulation 191; João Pedro Quintais and others, 'Copyright Content Moderation in the European Union: State of the Art, Ways Forward and Policy Recommendations' [2024] IIC - International Review of Intellectual Property and Competition Law; Alexander Peukert and others, 'European Copyright Society – Comment on Copyright and the Digital Services Act Proposal' (2022) 53 IIC - International Review of Intellectual Property and Competition Law 358.

[20] Article 3(j) DSA.

[21] Article 3(b) DSA: 'recipient of the service' means any natural or legal person who uses an intermediary service, in particular for the purposes of seeking information or making it accessible.

[22] Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights as amended by Directive 2011/77/EU of the European Parliament and of the Council of 27 September 2011 amending Directive 2006/116/EC on the term of protection of copyright and certain related rights (hereinafter "Term Directive").

[23] Term Directive, Article 1(1).

[24] Term Directive, Article 3(1) (rights of performers), 3(2) (rights of producers of sound recordings), 3(3) (rights of producers of the first fixation of a film).

[25] Term Directive, Article 3(1) second paragraph (50 years from making available of performances recorded otherwise than in a sound recording, 70 years from making available fixations of performances in a sound recording), 3(2) (70 years after publication or making available of a sound recording), 3(3) (50 years after first publication or communication to the public of films), 3(4) (50 years after first transmission of a broadcast).

[26] See for example the introductory phrase used in the CC0 waiver in section 2.

[27] See above section 3.2.1.

[28] See above section 3.2.1.

[29] See *Fisher v Brooker* [2009] UKHL 41 (establishment of co-authorship and claim of royalties to Whiter Shades of Pale by Procol Harum 38 years after release of the song)

[30] Recital 19 InfoSoc Directive.

[31] *See e.g.* Art. L121-1 French Intellectual Property Code (*Code de la propriété intellectuelle*); Article 16 Polish Copyright Act (*Ustawa z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych*).

[32] See section 2.2.2 and Annex.

[33] It seems it is a matter of national law to establish and regulate the interface between moral rights protection and exploitation of economic rights to so-called orphan works pursuant to Directive 2012/28/EU of the European Parliament and of the Council of 25 October 2012 on certain permitted uses of orphan works.

[34] Case C-263/18 *Tom Kabinet*, ECLI:EU:C:2019:1111.

[35] Case C-161/17 *Renckhoff*, ECLI:EU:C:2018:634.

[36] C-610/15 *Stichting Brein v Ziggo and XS4All*, ECLI:EU:C:2017:456.

[37] *See for example* Case C-466/12 *Svensson and Others v Retriever*, ECLI:EU:C:2014:76; Case C-348/13 *BestWater*, ECLI:EU:C:2014:2315; Case C-160/15 *GS Media v Sanoma*, ECLI:EU:C:2016:644; Case C-527/15 *Stichting Brein v Filmspeler*, ECLI:EU:C:2017:300.

[38] For example Case C-607/11 *ITV Broadcasting*, ECLI:EU:C:2013:147. *See also* Case C-306/05 *Rafael Hoteles*, ECLI:EU:C:2006:764; Case C-466/12 *Svensson and Others v Retriever*, ECLI:EU:C:2014:76; Case C-265/16 VCAST, ECLI:EU:C:2017:913.

[39] *See* Case C-637/19 *BY v CX*, ECLI:EU:C:2020:863.

[40] Tito Rendas, 'How Playboy Photos Compromised EU Copyright Law: The GS Media Judgment' (2017) J. Internet L. 20(11) 11 14. *See also* Case C-527/15 *Stichting Brein v Filmspeler*, ECLI:EU:C:2017:300.

[41] C-610/15 *Stichting Brein v Ziggo and XS4All*, ECLI:EU:C:2017:456.

[42] Earlier and subsequent CJEU cases on both secondary and primary communications require specific or actual knowledge of the unlawful nature of the content to establish liability; Joined Cases C-682/18 and C-683/1 *Peterson and Elsevier v YouTube and Cyando*, ECLI:EU:C:2021:503. *See also* Quintais, João Pedro, A New Liability Paradigm for Online Platforms in EU Copyright Law (May 22, 2025). In Governance of Digital Single Market Actors (Elgar Law 2025), Edited by Katja Weckström Maria Lillà Montagnani and Katarzyna Klafkowska-Waśniowska.

[43] PMÖD, case PMT 11706-15, judgment delivered 13.02.2017 (B2 Bredband).

[44] PMÖD, case PMÖ 7648-19, judgment delivered 1 October 2019 (Elsevier) concerning interim website blocking injunction; PMÖD, case PMT 13399-19, judgment delivered 29 June 2020 (*Telia dynamic injunction*) concerning final dynamic website blocking injunction. Cf. PMÖD, case PMÖ 9945-18, judgment delivered 6 February 2019 (*Telia*) concerning interim website blocking injunction, which was denied. *See also* Case C-314/12 *UPC Telekabel Wien v Constantin Film and Wega Filmproduktionsgesellschaft*, ECLI:EU:C:2014:192.

[45] Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, A European Data Strategy COM/2020/66 final (2020); Secretary-General of the European Commission, Commission Staff Working Document on the Common European Data Spaces SWD (2024).

[46] Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and

amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (hereinafter DA); Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act) (hereinafter DGA).

[47] European Commission: Directorate-General for Research and Innovation and Senftleben, M. R., Study on EU copyright and related rights and access to and reuse of data, Publications Office of the European Union, 2022, https://data.europa.eu/doi/10.2777/78973; Thomas Margoni et al 'Data Property, data governance and Common European Data Spaces' Computerrecht: Tijdschrift voor Informatica, Telecommunicatie en Recht (2023).

[48] (Margoni et al., 2023; Senftleben, 2022).