DELIVERABLE

Project Acronym: **Europeana Cloud**

Grant Agreement number: **325091**

Project Title: **Europeana Cloud: Unlocking Europe's Research via The Cloud**

D5.3 Europeana Cloud Access and Reuse Framework
(originally: Revised Europeana Licensing Framework)

Revision: 2.0

Authors:

Maarten Zeinstra (Kennisland)
Lisette Kalshoven (Kennisland)

Project co-funded by the European Commission within the ICT Policy Support Programme		
Dissemination Level		
P	Public	

Revision History

Revision	Date	Author	Organisation	Description
0.1	01-03-2014	Maarten Zeinstra Lisette Kalshoven	Kennisland	First version presented at the Europeana Plenary 2014.
0.5	01-06-2014	idem	idem	Initial Version for internal feedback.
1.0	01-03-2015	idem	idem	First version after extension of deliverable date incorporating feedback from EF, TEL and PSNC.
1.9	09-05-2015	idem	idem	Final version to be validated at the Europeana Cloud Plenary.
2.0	12-06-2015	idem	idem	Final version after extensive feedback.

D5.3 Europeana Cloud Access and Reuse Framework

D5.3 is formally named 'a Revised Europeana Licensing Framework', however due to the nature of the project this name does not reflect the work that needed to be done. Europeana will become one of the services that function on top of the infrastructure of Europeana Cloud. Therefore no changes to the Europeana Licensing Framework are required. However, the system described in the Description of Work required an Access and Reuse Framework. This deliverable reflects the principles guiding that work.

D5.3 has been long in the making, an initial version was written in early 2014, presented at the Europeana Cloud plenary 2014 in Athens. A period of extensive review brought the conclusion that there were several dependencies that the consortium needed to make decisions prior to finalising this deliverable. Most notably the work presented in D5.6. Work on the the Revised Europeana Licensing Framework was postponed until spring 2015.

After D5.6 was delivered in January 2015, Kennisland drafted an initial version that was circulated throughout relevant partners of the consortium. This led to extensive rewriting and rephrasing of the deliverable. The Europeana Cloud Access and Reuse Framework contains principles that govern access and reuse to Europeana Cloud.

On access to Europeana Cloud:
1. Data partners have full access control over the files they upload.
2. Data partners shall be able to grant other data partners and the general public read permissions to files.
3. Data partners shall be able to grant other data partners write permissions to files.
4. Data partners shall be able to grant other data partners delete permissions to files.
5. Data partner can request data to be persistent;
    a. Data partner that have write permission of files can make files persistent.
    b. The general public will be informed of the deletion upon requesting the files and contact information shall be provided by the Data Provider.

On rights statements of Europeana Cloud:
1. Rights statements are mandatory for all files when read permissions are granted to users other than the creator.
2. There is no default rights statement.
3. Different versions of the same file can have different rights statements.
4. Rights statements cannot be retracted;
    a. unless for more permissive rights statement.
    b. unless in accordance with the take-down policy.
5. We encourage Public Domain works to be labeled as such.

On technical metadata:
1. Data partners and the general public have read permission to technical metadata, once read permission to a file has been given to users other than the creator.
2. Available technical metadata will be released under a CC0 Public Domain Dedication waiver.

Future work on this deliverable will be to guide Work Package 2 on the implementation of these principles in technical framework of Europeana Cloud.

The appendix contains the Europeana Cloud Access and Reuse Framework as validated by the Consortium in the Europeana Cloud Plenary of June 2015.

Appendix 1 – Europeana Cloud Access and Reuse Framework

Europeana Cloud
Access and Reuse Framework
Version for Europeana Cloud Plenary (Edinburgh, Scotland 2015)

WP5: Legal, Strategic and Economic Issues

Maarten Zeinstra & Lisette Kalshoven (Kennisland)

Table of Contents

Introduction and background

Europeana Cloud allows data partners to efficiently store, share and provide access to digital cultural heritage. Europeana Cloud enables structural access to multiple data formats. It does not only store metadata about cultural objects (like europeana.eu) but it can store all sorts of additional files and information. It is part of the mission of Europeana Cloud, as it is of the Europeana Network, to create new ways for people to engage with their cultural history whether for work, learning or pleasure.

Europeana Cloud's services allow partners to perform rudimentary functions that can be expected from a cloud environment, such as:

- upload and download files;
- control and manage user authentication, access permissions & terms of (re)use of their files;
- allow others (other data partners and the general public) to enrich and annotate files, while keeping the original files intact;
- more efficient ways for delivering cultural heritage data to Europeana than in the current situation;
- support with interoperability issues;
- infrastructure for supporting data processing services needed as part of the standard aggregation workflow.

Additionally, all data partners benefit from trusted policy frameworks that enable continuity of existing standards for sharing files within cultural heritage.

Structural access and reuse rules are necessary to engage with this heterogenous rich set of cultural files. To structurally enable this access, balancing the institutions wishes with technical capabilities, it needs a framework that governs the way files are exchanged. The Cloud Access and Reuse Framework presented in this document defines the standards and best practices for sharing files stored in Europeana Cloud.

Access permissions within Europeana Cloud control who has read permissions, write permissions and delete permissions within Europeana Cloud. However, being able to see a file is often not enough for the general public. They want to be able to reuse culture. Europeana Cloud advocates this sharing and makes it easier. The access and reuse

framework follows this ambition.

This document is prepared based on the input of the Europeana Cloud consortium. It establishes the principles of the framework for access and reuse to and from this system. It outlines the legal agreements necessary to enable the exchange of files within the Europeana Cloud Services.

On behalf of Europeana Cloud WP5 (Legal, Strategic and Economic Issues):

- Maarten Zeinstra   mz@kl.nl
- Lisette Kalshoven   lk@kl.nl

PS: The images used in this document are crops from Kinderen der zee *by Dutch painter Jozef Israëls in 1872. The painting is in the public domain collection of the Rijksmuseum.*

Vocabulary

The list below presents key terms used in the document together with explanations of their meaning in the context of this document, in alphabetical order. These definitions are inspired but not equivalent to the Europeana Glossary[1] and additional definitions[2] developed within the Europeana Cloud Project.

- **Access Permissions** – Access Permission can refer to Delete Permission, Read Permission, and Write Permission.
- **Authorisation** – One or more Access Permissions that are granted to a Data Partner or the General Public.
- **Data Partner** – An organisation that is a member of Europeana Cloud. Data Partners are allowed to manipulate Files on Europeana Cloud, when they are Authorised to do so. Data Partners can allow third party services to manipulate files on behalf of Data Partners.
- **Delete Permission** – Granted Authorisation by a Data Partner to permanently remove a File.
- **General Public** – anyone who is not a data partner of Europeana Cloud or not logged into the Europeana Cloud services.
- **Europeana Licensing Framework (ELF)** – The framework of agreements, guidelines and terms and conditions that facilitates the supply, exchange, access to and use of metadata and content via Europeana.eu
- **File** – a File is the resource for storing information, a File is any digital document.
- **Intellectual Property Rights (IPR)** – Legislation that includes, but is not limited to, copyrights, related (or neighbouring) rights, and database rights.
- **Read Permission –** Granted Authorisation by a Data Partner to a Data Partner or General Public to view a File.
- **Technical Metadata –** All metadata that is created by the system or necessary for the system to operate is defined as Technical Metadata, including (local) identifiers, rights statements and the names of File creators.
- **Write Permission –** Granted Authorisation by a Data Partner to a Data Partner to copy a File within the system or update a File.

---

[1] Europeana Glossary http://pro.europeana.eu/glossary

[2] Additional definitions documented D2.2 Europeana Cloud Architectural Design
http://pro.europeana.eu/documents/1414567/2240207/D2.2+Europeana+Cloud+Architectural+Design?version=1.1

Providing access to your files

Europeana Cloud allows data partners to upload files. It allows control over access to these files, allowing other data partners and the general public to read – and in case of data partners – write, delete, and manage permissions over collections of files. How this access is managed and to which requirements they result in are described below.

As a data partner of Europeana Cloud you have control over who has access to your files. When you choose to, you can give several types of permissions to other data partners and the general public. These permissions are necessary to make the ecosystem of digital cultural heritage work. For example, if you want the general public to see your files on your website, they need to have direct link to that file. Also, if you want to share your non-public files with a specific other data partner, you can give them read permission, write permission and delete permission.

> *Requirement (Data Partner): I want to have control over who can access and reuse my files.*

The ability to easily share files is one of the main advantages of hosting your files in Europeana Cloud. Depending on which service built on Europeana Cloud you want to use, some permissions can be mandatory. For example, if you want your high-resolution images to be visible on Europeana.eu you need to give read permission to the general public to view it.

Sharing your files

When you first upload new files to Europeana Cloud you are the only person who has access permissions to them. For Europeana Cloud this is a method of managing uploading, and a way to upload files that are too sensitive to be shared with data partners and beyond, such as files containing information about living people. Europeana Cloud strongly encourages its data partners to share their files as openly as possible.

> *Requirement (Data Partner): I need to be the only one who has access permissions for files when they first enter Europeana Cloud. This way, I can manage uploads and evaluate what I want to share with data partners and beyond.*

Others can read your files (read permission), make copies or update files (write permission), and delete files (delete permission) only after the data partner explicitly gives one or more of these permissions.

> *Requirement (Data Partner): I need to share my files to specific people and institutions within and outside Europeana Cloud. This enables working together with other institutions in Europeana Cloud without having to share publicly. This also enables me to control the access to researchers or other platforms.*

Building on your files

All data partners can upload files based on existing files if they have read permission. This allows collaboration between different data partners and can allow platforms like Europeana.eu to transform your files into other formats (e.g. convert images into thumbnails and convert metadata into different formats).

Providing derivative files does not mean replacing older files, writing new files creates a copy, including the adaptations. Data partners that are granted delete permission on specific files can permanently remove files from Europeana Cloud.

> *Requirement (Data Partner): I need to collaborate with other data partners, building on my files, without losing the files I upload.*

Europeana Cloud wants to enable the use of cultural heritage files for research purposes. One important issue that holds back digital research is the lack of persistency in online sources (broken links). Therefore, Europeana Cloud allows data partners to make files persistent and request persistency from files that are not owned by other data partners. Data partners can grant this request.

> *Requirement (Researcher): I need permanent links to files shared in the Cloud to keep my research validated.*

It can be necessary to delete files from the Cloud that have been marked as persistent. The two most common use cases for this would be copyright infringement and infringing on privacy laws. Therefore, deletion of persistent files will be possible when it is in line with the Europeana Cloud take-down policy.

Principles

1. Data partners have full access control over the files they upload.
2. Data partners shall be able to grant other data partners and the general public read permissions to files.
3. Data partners shall be able to grant other data partners write permissions to files.
4. Data partners shall be able to grant other data partners delete permissions to files.
5. Data partner can request data to be persistent;
   a. Data partner that have write permission of files can make files persistent.
   b. The general public will be informed of the deletion upon requesting the files and contact information shall be provided by the Data Provider.

Rights statements

The above outlines how files can be accessed on Europeana Cloud. Access meaning reading, writing and deleting files. These permissions can be given to other data partners within Europeana Cloud and to the general public. Whether these other data partners and the general public can *reuse* the files they've been given access to them in the legal sense depends on the IPR status of those files. To communicate this status, Europeana Cloud includes rights statements. These rights statements are mandatory when read access is provided to data partners who are not the original creator of the files or to the general public.

> *Requirement (Data Partner): It is important that we have clear and coherent rights information available in Europeana Cloud.*

The importance of reuse

Europeana Cloud encourages reuse. Enabling reuse is enabling to build upon Europe's shared culture. It is what allows researchers to mix databases, what allows the creative industries to create new culture and what entices the general public to fully experience what cultural heritage institutions have to offer.

> *Requirement (Europeana Cloud project): We want to promote reuse of cultural heritage in Europeana Cloud to enable research, creative industries and education to benefit from our culture.*

Making files available for reuse, however, is not always possible or desirable. IPR, including copyright, restrict reuse without the explicit consent of the rights holders. Also, It might not be desirable or possible to allow reuse for files that include information covered by privacy legislation.

Data partners of Europeana Cloud need to provide rights statements to each uploaded file when this file is made available to other data partners or the the general public. This also means that different versions of the same file can have different rights statements. An example of this can be a data partner creating a rendition of a public domain work in which she adds sufficient originality to attract copyright. In that case the data partner needs to have the ability to apply a rights statement of the work she created. She will not be able to change

the rights statement of the original version that she adapted.

These factors explain why it will not be possible to have a default rights statement or inheritance of rights statements.

Available statements

Europeana Cloud will have a controlled vocabulary of rights statements. Initially, this list follows the structure of the ELF. The Europeana Foundation developed five rights statements and allows for a series of eight legal tools developed by Creative Commons. Future developments include an expansion of the possible rights statements, following the shared namespace of Rights statements http://rightsstatements.org/ that is being developed by Europeana, the Digital Public Library of America and Creative Commons.

> *Requirement (Data Partner): We need clear rights statements that fit the needs of our collections.*

Rights statements are not easily retractable, they can only be replaced for more open statements, or retracted in accordance with a take-down policy. This is needed to enable protection for reuse of the files. For example, if a sound file was published under a Creative Commons Attribution license, and someone creates a new musical work based on this. It would bring the derivative work's legal status in question as the rights statement is altered to a more restrictive license afterwards.

When all restrictions due to IPR of a file have expired an object enters the public domain. This means that data partners or others cannot control the reuse of a work through copyright and similar rights restrictions. Europeana Cloud follows the principles of the Europeana Public Domain Charter[3] and encourages its data partners not to mark files as still restricted by intellectual property when this is no longer the case.

---

[3] See http://pro.europeana.eu/get-involved/europeana-tech/europeana-tech-events/the-europeana-public-domain-charter

> *Requirement (Europeana Cloud project): We stand for a thriving public domain and encourage use of the Public Domain Mark where IPR protection is not applicable.*

Principles

1. Rights statements are mandatory for all files when read permissions are granted to users other than the creator.
2. There is no default rights statement.
3. Different versions of the same file can have different rights statements.
4. Rights statements cannot be retracted;
    a. unless for more permissive rights statement.
    b. unless in accordance with the take-down policy.
5. We encourage Public Domain works to be labeled as such.

Access and reuse of technical metadata

Europeana Cloud keeps track of what is stored in its system by adding technical metadata to files. Technical metadata only contains descriptive information about files. Information that is considered technical metadata includes but is not limited to:

- global ID
- local ID
- type of file representation (e.g. EDM, MARC, JPG, ...)
- filename
- provider of the files
- assignment to data set(s)
- date of upload to Europeana Cloud
- access statement
- rights statement

Data partners and the general public have read access to technical metadata when the underlying file is available to them. Otherwise Europeana Cloud cannot be used properly. Maintaining IPR claims on technical metadata results in complex agreements with data partners and the general public which Europeana Cloud wants to avoid. This does not mean that data partners will always have access to files stored in Europeana Cloud.

Technical metadata needs to be reusable to enable the Europeana Cloud infrastructure and services to function. This technical metadata will therefore be released under a Creative Commons zero Public Domain Dedication waiver (CC0) once the file has been shared with anyone other than the original uploader (data partner).[4]

> *Requirement (Data Partner): We need easily reusable technical metadata in order to work with the system. This includes incorporating information about files from other data partners that we have access to.*

---

[4] see https://creativecommons.org/publicdomain/zero/1.0/

CC0 enables Europeana Cloud to waive rights in this technical metadata and thereby place them as completely as possible in the public domain, so that others may freely use this information without restriction under copyright or database law.

Principles

1. Data partners and the general public have read permission to technical metadata, once read permission to a file has been given to users other than the creator.
2. Available technical metadata will be released under a CC0 Public Domain Dedication waiver.

Take-down policy

A Europeana Cloud take-down policy is necessary as mentioned before in this document. This policy will be written by WP5 to make certain that Europeana Cloud both provides access to our heritage, and at the same time protect our data partners by making it possible to delete files when necessary. The two most likely scenarios are infringements of IPR and infringement of privacy.

> *Requirement (Data Partner): I need to be able to delete files when we are infringing copyright or privacy rights in Europeana Cloud.*

Infringements of IPR can occur when a data partner has unlawfully provided read permission to a file, and/or when an incorrect rights statement was provided. Privacy laws can be infringed when files with personal information are released when that should not have been in the local jurisdiction. These cases call for a change in the access and reuse permissions of the affected files.

When Europeana Cloud receives a take-down request for a file, it will be taken down immediately. The request is then communicated to the data partner who can take appropriate action.

A notice will remain at the URL of the file stating that this file was deleted, to allow a permanent reference for the use of research. This notice will include information on the

providing data partner.

Take-down of persistent files

When a data partner to Europeana Cloud sees the need for deletion of a record that has been made persistent (see 'Providing access to your files') they will request deletion from an administrator. The request will be processed on a case-by-case basis by Europeana Cloud and the data partner within a timely manner. When the request adheres to the take-down policy it will be either deleted or read permission will be removed.