

## **ERASysAPP Data Sharing Policy**

Principles adopted by the ERASysAPP  
community for sharing data, models and  
processes

16 July 2013

# ERASysAPP Data Sharing Policy

## Summary

The aim of this document is to set the principles to be adopted for sharing the data, models experimental designs and data processing workflows generated by the ERASysAPP community. The principles should provide the foundation for a common policy to be built in consultation with the ERASysAPP community, the ERASysAPP-DMP (Data Management Project) team, and the funding organisations involved in ERASysAPP.

## Introduction

At the heart of the ERASysAPP initiative is the aim to pool European research capacities and know-how of the systems biology community. In addition to the benefits of the transnational collaboration taking place within each ERASysAPP project, the ERASysAPP initiative has the ambition to provide an opportunity to researchers to increase the scope for their work, to benefit from access to valuable data resources and to be better equipped to address complex scientific challenges through the implementation of a data sharing platform, the operation of which is backed by a data sharing policy.

Data represent an asset, produced in the context of a specific research subject/area, related to a particular technology used and linked to a specific hypothesis. The value to those producing the data is therefore very high. However, the exploitation of these data is, at present, limited to a specific group of researchers working in a specific subject. In reality, full exploitation of these data is not possible as the scale of the data generated often exceeds the human capacity, resources and time scales to be exploited by their own producers. Full exploitation of these data through the integration with other data, models and technologies is often hampered.

Funding bodies and journals are favouring more and more the release of data to maximise the value of the information and to accelerate scientific progress. Access to data, models, protocols, experimental designs, algorithms and data processing workflows is necessary to ensure the reproducibility of scientific results. Early data release, i.e. pre-publication, is being encouraged but producers need recognition for the value of their data in a similar way that authors of research publications get citation. The citation of unique data identifiers, i.e. DOIs (Digital Object Identifiers), is developing as an appropriate mechanism to give credit to data producers in a similar way to publication credits (Nature Genetics [2009] vol. 41, number 10, p. 1045).

The ERASysBio call "Systems Biology of Microorganisms" pioneered the establishment of a formal data management structure linking 89 research groups working in systems biology of microorganisms. This was a complex task and a process that started with the establishment of a web-based platform for the exchange of data, models and processes in July 2008, with funding from BBSRC and BMBF. Later, a "SysMO Data Sharing Policy" was created to define the rules, rights and duties linked to the use of this Data Management System. It was prepared by Gabriela Pastori (BBSRC, UK) with assistance by Chris Rückert (PtJ, Germany) and agreed among the funded scientists in both SysMO calls, the SysMO Scientific Advisory Board and the SysMO funding organisations.

This generic document bases on the SysMO Data Sharing Policy

## ERASysAPP-Data Management Project

The ERASysAPP-DMP will provide a horizontal structure for the management of data, models and processes within- and inter-consortia, and aims at their progressive exchange and use across the borders of projects and nations. The ERASysAPP- data management will encompass common concepts for data storage, data and model exchange and sharing as well as communication between the scientific groups in the ERASysAPP community. To maximise its benefits beyond ERASysAPP, ERASysAPP-DMP will provide an integrated platform for the dissemination of the results of the ERASysAPP projects to the scientific community.

The individual project partners in ERASysAPP are working towards different research outcomes and represent a cross-section of different research areas. ERASysAPP-DMP aims at supporting and managing this diversity and promoting a shared understanding across the community by using the same technologies.

ERASysAPP-DMP aims to devise a progressive and scalable solution, subsequently referred to as “ERASysAPP-DM platform” to the data management needs of the ERASysAPP initiative, that:

- facilitates and maximises the potential for data exchange between ERASysAPP research groups;
- maximises the ‘shelf life’ and utility of data generated by ERASysAPP researchers;
- provides an integrated platform for the dissemination of the results of the ERASysAPP projects to the scientific community; and
- facilitates standardisation of practices in systems biology for the interfacing of modelling and experimentation.

## **Why a policy for data sharing?**

The ERASysAPP-DM platform can only operate optimally if backed by a common policy for sharing the data, models and processes generated by the ERASysAPP community.

This policy facilitates the deposition and exchange of data (metadata, SOPs, spreadsheets) and models, and maximises the use and functionality of the ERASysAPP-DM platform. The document consists of collaboration agreements and non-disclosure agreements, and the policy covers the following areas:

- storage and retention of data within each ERASysAPP consortium;
- storage of data in public repositories;
- deposition and retention of data (metadata, SOPs, spreadsheets) and models in the ERASysAPP-DM platform;
- access to data and models stored in the ERASysAPP DM platform by other ERASysAPP consortia, and by the wider scientific community;
- lifespan of ERASysAPP-DM platform and long-term sustainability.

The aim of this document is to set the principles to be adopted by the ERASysAPP community.

## **OECD principles for access to research data from public funding**

Since their release in 2007, the OECD principles of data sharing are being progressively adopted by research communities and their organisations, and implemented by funding agencies, international organisations and scientific journals.

### ***What is the OECD?***

The Organisation for Economic Co-operation and Development is a unique forum where governments of 34 democracies work together to address the economic, social and environmental challenges of globalisation. The organisation provides a setting where governments can compare policy experiences, seek answers to common problems, identify good practice, and work to coordinate domestic and international policies.

The OECD member countries are: Australia, Austria, Belgium, Canada, Chile, the Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Israel, Italy, Japan, Korea,

Luxembourg, Mexico, the Netherlands, New Zealand, Norway, Poland, Portugal, the Slovak Republic, Spain, Sweden, Switzerland, Turkey, the United Kingdom, and the United States.

### **OECD Principles**

The OECD principles for access to research data from public funding were released in 2007 and can be found at <http://www.oecd.org/dataoecd/9/61/38500813.pdf>.

#### **Openness**

Open access to research data from public funding should be easy, timely, user-friendly, and preferable Internet-based.

#### **Flexibility**

Flexibility takes into account the rapid changes in information technologies, the characteristics of each research field, and the diversity of research systems, legal systems and cultures of each member country.

#### **Transparency**

Information on research data should be internationally available in a transparent way, ideally through the Internet. Transparency is a necessary requirement for the reproducibility of scientific results and to allow further exploitation of released data.

#### **Legal conformity**

Data access arrangements should respect the legal rights and legitimate interests of all stakeholders. Access might be limited due to:

- National security: intelligence, military activities, political decisions may be classified.
- Privacy and confidentiality: data on human subjects and other personal data are subject to national laws. Anonymisation should be considered.
- Trade secrets and IPR: data on or from businesses that contain confidential information.
- Protection of rare, threatened or endangered species: there might be legitimate reasons to restrict access to data on location of such biological resources.
- Legal process: data under consideration in legal actions.

#### **Protection of Intellectual Property**

Data arrangements should consider the applicability of copyright or of other intellectual property laws that may be relevant to publicly funded research databases. The involvement of the private sector in a public-private partnership should not, in itself, be used as a reason to restrict data access.

#### **Formal responsibility**

Access arrangements should promote explicit, formal institutional practices, such as development of rules and regulations, regarding the responsibilities of the various parties involved in data-related activities: authorship, producer credits, ownership, dissemination, usage restrictions, financial arrangements, ethical rules, licensing terms, etc.

#### **Professionalism**

Arrangements for the management of research data should be based on the relevant professional standards and values embodied in the codes of conduct of the scientific communities involved:

- The use of codes of conduct for professional scientists and their communities could help simplify and reduce the regulatory burden placed on access.
- Mutual trust between researchers, between researchers and their institutions and other organisations plays an important role.
- In current research practice, the initial data-producing researcher or institution is sometimes rewarded with temporary exclusive use of the data. The rules for such incentive should be developed by the funding sources in co-operation with the affected research communities.

### **Interoperability**

Technological and semantic interoperability is a key consideration in enabling and promoting international and interdisciplinary access to and use of research data. The standards employed should be explicitly mentioned.

### **Quality**

The value and utility of research data depends, to a large extent, on the quality of the data themselves. When such standards do not exist, institutions and research associations should engage with their research communities on their development.

### **Security**

Specific attention should be devoted to supporting the use of techniques and instruments to guarantee the security and integrity of research data.

### **Efficiency**

One of the central goals of promoting data access and sharing is to improve the overall efficiency of publicly funded scientific research to avoid the expensive and unnecessary duplication of data collection efforts.

### **Accountability**

The performance of data access arrangements should be subject to periodic evaluation by user groups, responsible institutions and research funding agencies.

### **Sustainability**

Due consideration should be given to the sustainability of access to publicly funded research data as a key element of the research infrastructure.

## **National data sharing policies in ERASysAPP funding organisations**

### **Austria – Austrian Federal Ministry for Science and Research (BMWF)**

Data policies are in preparation.

### **Cyprus – Research Promotion Foundation (RPF)**

Collection and processing of personal data included in proposals submitted at RPF and funded research projects, is carried out according to the Processing of Personal Data (Protection of the Individual) Law of 2001 and RPF's Regulation on Collection, Processing and Use of Personal Data. RPF's Regulation is posted on RPF's website.

### **Germany - Project Management Jülich (PtJ) and Federal Ministry of Education and Research (BMBF)**

Institutions funded by BMBF/PtJ are expected to retain their data in original form for a period of 10 years after the completion of the research project. There is no further detailed data policy. Rules, duties and rights have to be implemented in the collaboration contracts of the individual consortia or in such contracts among consortia. Participation in central data management approaches can be made mandatory if it is included into the so-called "Nebenbestimmungen" (additional conditions) to the grant contract.

### **Estonia – Estonian Research Council**

The Estonian Research Council doesn't have any Data Sharing Policy yet. However a document is in preparation.

### **The Netherlands - Nederlandse organisatie voor gezondheidsonderzoek en zorginnovatie (ZonMw) and Netherlands Organisation for Scientific Research (NWO)**

In their grant terms and conditions ZonMw and NWO (Netherlands Organisation for Scientific Research)

state that data from funded projects must be open for re-use in future research. Therefore, applicants must submit a data management plan early during their project. The minimal condition is that the data must be traceable and stored sustainably. In addition, ZonMw and NWO stimulate researchers to perform their research by making use of existing data.

In the case of ERASysAPP, ZonMw and NWO require at the minimum that project leaders and project researchers distribute and deposit their data according to the guidelines and agreements of the international ERASysAPP collaboration of funding agencies and research consortia

### **Norway - Research Council of Norway (RCN)**

The Project Owner or Principal Investigator shall store the final report and project data in a safe and secure manner for at least 10 years after the expiry date of the contract period. The Project Owner is required to ensure that the data are stored safely and remain accessible even in the event the Project Owner itself is closed down or otherwise ceases to exist.

The Project Owner is under obligation to ensure, in so far as possible, that peer-reviewed scientific articles based on research wholly or partially funded by the Research Council are stored in appropriate, open-access digital archives. It is presumed that such storage does not in any way conflict with the author's academic and legal rights".

### **Romania – Unitatea Executiva pentru Finantarea Invatamantului Superior, a Cercetarii, Dezvoltarii si Inovarii (UEFISCDI)**

The documents and data from a publicly funded research project must be stored 3 years after the end of a project, unless there is a specific regulation / law governing the results obtained that require a longer period (e.g. IPR, national security, etc.) or otherwise agreed among partners.

### **Spain – Ministry of Science and Innovation (MICINN)**

Researchers and research institutions participating in ERASysAPP and funded by MICINN are required to adopt the common strategy elaborated by ERASysAPP-DMP with regard to standardisation, management, storage and dissemination of data. This requirement is explicitly included within the conditions of each particular grant contract.

### **Sweden - Vetenskapsrådet**

At the moment there are no regulations in Sweden concerning data sharing. Researchers receiving funding have to follow the open-access regulation as mentioned in the national annex (also see link:

<http://www.vr.se/inenglish/researchfunding/applyforgrants/generalconditionsforgrantapplications/openaccess.106.5adac704126af4b4be280007766.html>)

### **United Kingdom – Biotechnology and Biological Sciences Research Council (BBSRC)**

In April 2007, BBSRC launched its new data sharing policy, setting out expected standards of data sharing for BBSRC-supported researchers. The policy states that BBSRC expects research data generated as a result of BBSRC support to be made available with as few restrictions as possible in a timely and responsible manner to the scientific community for examination and use. The policy aims to achieve the sharing of data in a both a timely and scientifically appropriate manner.

All research proposals submitted to BBSRC since 26th April 2007 must include a statement on data sharing. This should include concise plans for data management and sharing or provide explicit reasons why data sharing is not possible or appropriate.

In addition, in line with BBSRC guidance on good scientific practice, researchers are expected to ensure that data are:

- maintained for a period of 10 years after the completion of the research project;
- in suitable accessible formats, using established standards where possible;
- available on request.

ERASysAPP UK grant holders are required to comply with BBSRC Data Sharing policy, and with

the specific data management and sharing policies being developed under the ERASysAPP initiative. Grant holders are also required to contribute to the operation of the ERASysAPP-DMP platform, and to nominate a representative from each consortium to participate as a member of the ERASysAPP Data Management Group, and at least one postdoctoral scientist from the consortium to act as Project Area Liaison (PAL).

## **ERASysAPP principles for access to research data and secure storage**

### **Definitions**

#### **What are 'data' in the ERASysAPP community?**

There are different types of assets to be shared by the ERASysAPP projects and by the wider systems biology community:

- data generated by high throughput experiments; and
- data arising from low throughput, cumulative experiments, in the form of:
  - raw data, i.e. single pieces of data belonging to a larger data series, non-replicated data, non-quantified data;
  - experimental results, i.e. reliable, quantified and repeated data series, including high throughput data;
  - calculated data, i.e. involving further analysis of raw data;
  - image data;
- data arising from biological modelling;
- models generated by systems biology approach;
- model results;
- parameterisations of models;
- validation data for models;
- validation results for models;
- metadata, i.e. data providing information about one or more pieces of data;
- processes used to design the experiments, generate the data, and generate the models, i.e. standard operation procedures, spreadsheets, workflows.

Hereafter we refer to all of these types of ERASysAPP assets as *data*.

Note: grey data, i.e. lab notebooks, preprints, other data arising from the projects which are not stored in an electronic format, are not covered by this policy.

**ERASysAPP-DMP** refers to the data sharing project.

**ERASysAPP-DMP Team** refers to the research and development team developing the software.

**ERASysAPP-DM platform** refers to the software application.

**Data owner** refers to the principal investigator and their institution holding a ERASysAPP grant (i.e. a national grant given in reference to an ERASysAPP call) under which the data are generated, and that are ultimately responsible for the assignment of access settings of such data.

**Project partner** refers to an individual research group in a transnational collaboration funded by a common call for research projects (the single group in a collaborative project).

**Project** refers to a group of scientific partners working together and funded by a common transnational call for research projects (the collaborative project).

**Funding initiative** refers to a national or transnational call for research projects funded by public organisations and aiming at generating multipartner research collaborations in a given strategic

area (the ERASysAPP call).

**Data Management Group** refers to a group of representatives of all projects in data management and data sharing relevant subjects. The group will elect a chair and a vice-chair person.

## 1. General Principles of Data Exchange

### 1.1. Storage and retention of data within each ERASysAPP project

Data generated by research groups within each project should be visible as metadata to all members within the consortium with immediate effect. Members of the consortium must give credit and cite the use of the data in all publications, and according to the terms and conditions of the consortium's collaboration agreement.

### 1.2. Deposition and retention of data (metadata, SOPs, spreadsheets) and models in ERASysAPP-DM platform

Data generated by research groups should be made visible in ERASysAPP-DM platform at the earliest opportunity. Data must be categorised, e.g. as raw, validated, ready for publication, when deposited in the ERASysAPP-DM and new versions of the data be created as "data is polished" or "updated". Overwriting datasets is not permitted.

### 1.3. Storage of data in public repositories

Whenever possible, data generated by the ERASysAPP consortia should be deposited in public repositories at the time of publication. Here standard formats should be used when applicable. The following public repositories are recommended:

- ArrayExpress or GEO for transcriptomics data
- PRIDE for Proteomics data
- BioModels Database or JWS Online Model Database for computational model data (SBML)
- See Biosharing.org for more repositories

Note: for genomic data, the NCBI trace file archives are generally used by the community (<http://www.ncbi.nlm.nih.gov/Traces/trace.cgi>). However, NCBI is now closed to new submissions so it is recommended that genomic data is archived in the European Nucleotide Archive (<http://www.ebi.ac.uk/ena/>). In any case, the ERASysAPP community should judge if this fulfils their needs and could be used as their public archive.

### 1.4. Standards

The ERASysAPP community use a range of standards for data exchange. First, Minimum Information guidelines should be consulted to ensure provision of all information necessary to make data sets reusable. All publicly provided data should contain the information defined in the according MI, e.g. MIAME for microarray experiments, MIAPE for proteomics experiments, or MIRIAM for computational models. Second, the data itself (see 1.3) should be annotated with ontological terms from biological ontologies. Ontologies recommended by the OBO Foundry are to be preferred, e.g. Gene Ontology, MGED, SBO.

### 1.5. Intellectual Property Rights

The ERASysAPP funding organisations adhere to the OECD principles. Where data generated by ERASysAPP projects are capable of industrial or commercial application, their owners shall provide for its adequate and effective protection in conformity with the project's Consortium Agreement. The involvement of the private sector in the project should not, in itself, be used as a reason to unduly restrict data access, recognising the needs of all partners to protect intellectual

property.

#### *1.6. Lifespan of ERASysAPP-DM platform and long-term sustainability*

It is expected that at the end of its funding, ERASysAPP-DM platform will contain a significant number of data and assets representing a valuable resource to the scientific community. An assessment of the quality and value of ERASysAPP-DM platform will be performed by an expert panel at the end of the funding period. Should the assessment be favourable, the ERASysAPP-DMP team with ERASysAPP funding organisations will be exploring ways towards the long-term sustainability of this resource.

The ERASysAPP scientific community has a key role to play by contributing to build ERASysAPP-DM platform as a valuable resource operating under the ERASysAPP data sharing principles. The expert panel will assess the responsiveness and commitment of the ERASysAPP community to the opportunities offered by this resource.

## **2. Responsibilities of the ERASysAPP-DMP Team**

This section outlines the responsibilities and commitments of the ERASysAPP-DMP Team.

### *2.1. ERASysAPP-DMP guarantees that it will take every reasonable care that data is held securely*

The ERASysAPP-DMP team will ensure that reasonable precautions are taken that data, as well as personal details of the users, activity logs, are stored in a secure manner.

### *2.2. All data will be incrementally backed up daily, with an off-site backup stored at least once a week*

All data, when stored centrally in the ERASysAPP-DM platform, are incrementally backed up during a regular nightly task. This backup is stored securely to a separate, with an off-site back up being done weekly.

### *2.3. ERASysAPP-DMP will not reveal information about data marked as private without the author's consent, other than for gathering coarse statistics on quantity and volume or as a result of being embargoed*

ERASysAPP-DMP users should be able to register data with ERASysAPP-DM platform with the confidence that the sharing permissions they have selected will be respected. Therefore, ERASysAPP-DMP can guarantee that it will not reveal data that would otherwise be hidden. This only applies as specified in 4.1. After this point, all data should be public.

For the purposes of promoting ERASysAPP-DMP, verifying the compliance of the ERASysAPP projects with this policy or to satisfy funding requirements, it may be required to publish statistics on the volume and quantity of data, but this will always be coarse grained.

In the case of technical failure, every effort will be made to resolve the problem as swiftly as possible, and if necessary ERASysAPP-DMP will take the system offline during the period between becoming aware of a problem and resolving it.

### *2.4. ERASysAPP-DMP will not delete ERASysAPP member user accounts or their data, or intentionally block them, as long as they adhere to the terms of acceptable use. This holds true even if a user changes their relationship with ERASysAPP.*

A user should be able to register data with ERASysAPP-DM platform with confidence that this

data will continue to be available to them regardless of their relationship to the ERASysAPP consortia. Their user account and profile will also remain available to them. The ERASysAPP-DMP is committed to keep all data stored in ERASysAPP-DM platform for 10 years from the end of the ERASysAPP-DMP project, i.e. 2028. Appropriate means to preserve the data beyond 2024 will be explored so that all valuable assets are secured.

Only in the exceptional case that users have seriously violated ERASysAPP-DMP terms of acceptable use, and reported to the Data Management Group and ERASysAPP funding organisations, their access to the ERASysAPP system will be locked.

ERASysAPP-DMP adheres to the Terms of Acceptable Use adopted by the Education and Research

Network JANET: <http://www.ja.net/company/policies/janet-aup.html>

*2.5. If a User leaves or moves to another project or funding initiative, then data that is not authored or contributed by them but is shared within that project may no longer become accessible.*

Users should understand that the nature of the sharing permissions means that there is data that could be accessible within their project that is hidden outside of their project. Should a user move from one project to another, or leave ERASysAPP altogether, then such data would become unavailable to them. If a user leaves a project, it is expected that the user and participants in the project will discuss whether access could be granted to the user in such circumstances. If access is granted to the user, the terms of such access to the project data must be agreed between project participants. In case of conflict, these discussions should be mediated by the DMG.

### **3. Responsibilities of the ERASysAPP Projects and Members**

This section outlines the responsibilities and commitments of the ERASysAPP-DMP users and projects.

*3.1. ERASysAPP members will make data available to ERASysAPP-DMP, either through their internal system or through a direct upload, whenever data is produced and is of reasonable quality. This may be marked hidden if necessary.*

Data produced within ERASysAPP has been funded through public money, and is of scientific value beyond the lifetime of ERASysAPP. All ERASysAPP members and projects are expected to upload their data to the ERASysAPP-DM platform, or make it available to it.

#### *Before publication*

Researchers are expected to make their metadata accessible to the ERASysAPP community six months after being produced.

Data that are not published and/or for which publication is not planned have to be made available at the end of the project funding **at the latest**, i.e. the day after the project expires. As ERASysAPP projects are funded by national funding organisations, the end date of the project refers to the end of the project partners' funding.

Projects may use creator's privileges on specific aspects of their data for up to 18 months after the project ends, enabling them to keep data restricted until expected or pending publications can be released. This can be done by placing a flag on these data to allow scientists to exploit their own discoveries before others benefit from reuse (see section 4).

#### *After publication*

All data generated by research groups should be accessible to the public via ERASysAPP-DM platform after the publication of the data (see 3.2). Only the last version of the data will be available and accessible. Previous versions will be made visible (of course, previous versions can be made available and accessible by the owner).

*3.2. ERASysAPP members will always make data publicly available if it is related to or involved in a publication or scientific claim.*

If data has been used as a basis of a scientific publication or other scientific claim, then it should be made available for peer review and validation. ERASysAPP members and projects are encouraged to make such data publicly available through ERASysAPP-DM platform. Before publication, data uploaded to ERASysAPP-DM platform may remain hidden, or restricted to viewing only by other members of the same project.

*3.3. ERASysAPP members are responsible for any content that they register with ERASysAPP-DMP. ERASysAPP- DMP may make copies for operational purposes.*

Ultimately, ERASysAPP members are responsible for content that they provide as there is no “Approval” or “Mentoring” system. Content registered should meet with ERASysAPP-DMP’s terms of a cceptable use.

Data which are not shared can be withdrawn, i.e. deleted. Once data are shared, this is not allowed anymore

Overwriting former versions of content with improved updates is not permitted. Rather, new versions of the data will be uploaded. Former content will persist as versions for operational purposes, such as incremental backups, and for users utilising such versions. These versions are made in accordance to ERASysAPP-DMP’s commitment to keeping data private and secure (see 1.1). The different versions must be labelled with version related information, such as inaccurate, current final, improved/corrected by follow-up version.

Data will not be removed once a project has finished and any creator’s privilege rights have expired (see section 4).

#### *3.4. Researcher leaving an ERASysAPP project*

When a researcher contracted under a ERASysAPP project (PhD student, Postdoctoral Scientist) leaves such project and/or the ERASysAPP funding initiative, the responsibility for the data assets generated by that researcher are automatically transferred to their supervisor, i.e. the head of the Project Partner group, or institution, according to national regulations.

In many ERASysAPP countries, projects are awarded to the institution rather than to the principal investigator. In this case, when a researcher leaves their institution, it is expected that appropriate arrangements will be made between such institution and the principal investigator holding the grant. These arrangements would either allow the principal investigator to take the grant with them to the new institution or allow the grant to be transferred to a new principal investigator nominated by the institution.

It is expected that appropriate arrangements between the institution and the principal investigator will be made so that the institution is granted access to the data generated by the project, both while the principal investigator is working at the institution and after the principal investigator moves to a new institution.

## **4. Public Release of Data and Creator’s Privilege**

*4.1. All data from finished projects should be made available to the scientific community.*

In cases where data are to be published after the end of the project, ERASysAPP projects can set a flag on these data to allow them a period of creator’s privilege of up to 18 months (see 3.1).. This will enable scientists to finish analyses and publish their data before others benefit from it. Once this creator’s privilege of 18 months after the end of the project has expired, data that have

been previously flagged will be automatically released into the public domain.

To facilitate dissemination and enhancing the value of the data beyond ERASysAPP within the scientific community, all data will become publicly accessible after a period of 18 months beyond the associated projects completion date. In the unusual scenario that more than one project has been involved in the production of that date, 18 months beyond the later completion date will be used.

Once creator's privilege expires, data that were once indicated as being flagged, i.e. hidden, will have their access restrictions automatically relaxed and become publicly accessible. The end of creator's privilege will be communicated to the data owner though no specific permission will be sought from the data owner at this stage.

Once creator's privilege expires, it will not be possible to edit the data or their metadata. Metadata may be modified only by internal processing systems; for example if there are improvements made to metadata extraction or presentation requiring a reprocessing of the data.

In exceptional cases, ERASysAPP projects may request an extension of creator's privilege beyond 18 months. A request for an extension of creator's privilege must be submitted to the ERASysAPP Data Management Group in the first instance (see 4.2), accompanied by a justification and supporting evidence.. The ERASysAPP Data Management Group will forward the request to the ERASysAPP Call Office together with a recommendation on why such privilege should be granted or should not. A final decision will be taken by the ERASysAPP funding organisations.

*4.2. Under exceptional circumstances, users may be able to delay the release of their data through a written request, which must be recommended by the ERASysAPP Data Management Group (DMG), as regulated in 4.1.*

There might be exceptional cases where a user, or project, requires an extended period of creator's privilege, e.g. patent application. In such a case, a written request should be submitted stating the reason for requesting more time. This justification must be accompanied by evidence, i.e. patent application, paper manuscript and letter from journal, etc, otherwise it will not be considered. The data will remain private whilst the written request is considered by the ERASysAPP- DMG. If such a request fails, then the data is publicly released. If such request is successful, the status of the data remains as its original status, or one described within the written request.

It is the duty of the ERASysAPP DMG to critically review the declarations and ask the data creators for clarification if necessary. In exceptional cases, the DMG may require access to the metadata or even the data. To protect IP, the DMG member will only access the data after signing a non- disclosure agreement with the data owner. The DMG will submit recommendations to the ERASysAPP call office. ERASysAPP funding organisations, in consultation with the ERASysAPP Scientific Advisory Board (SAB), will make a final decision.

*4.3. Use of data requires permission by the owner.*

Regardless of whether the data are published or not, potential beneficiaries of the data from ERASysAPP-DM platform are expected to notify the owners if they wish to use the data and submit a request via ERASysAPP-DM platform. Beneficiaries must give credit and cite the use of the data in all publications or offer joint authorship. This may lead to new collaborations between the new users and the data owners. Appropriate terms and agreements must be in place from the start of such collaboration. These terms must be set by the parties involved in the collaboration. Publications including supplementary data stored in ERASysAPP-DM platform must indicate the sources of such data, preferably via DOI or, alternatively, a ERASysAPP-persistent identifier.

DOIs provide a better alternative to URLs as they secure the information linked to it even if this information changes location. The current policy does not impose DOIs as the norm. It is assumed that if DOIs are created, these will be generated while preparing data for publication and will effectively be in the public domain when the paper is published. The DOI is nevertheless accessible to the public via the DOI registry. As for other data, e.g. sequences, it is assumed that

the value of the publication is in how the author(s) make use of the data rather than the data itself. As there is a fee associated to setting up a DOI, a viable alternative to these is the creation of a ERASysAPP-persistent identifier on ERASysAPP-DM platform with similar permission rules as for data.

## **5. Modification of this Sharing Policy**

This sharing policy might require modifications in the future. Such modifications will base on discussions between the ERASysAPP Data Management Group, the ERASysAPP-DMP team, the Scientific Advisory Board of the ERASysAPP call and the representatives of the national funding organisations (the ERASysAPP Executive Board). While a consensus among all participants will be attempted, non-consensus decisions underly a veto by the ERASysAPP Executive Board

END