EPOS ERIC

DIGITAL ASSETS MANAGEMENT POLICY

EUROPEANPLATEOBSERVINGSYSTEM

Design Barbara Angioni

ERIC established by the European Commission
Implementing Decision 2018/1732

EUROPEANPLATEOBSERVINGSYSTEM

EPOS ERIC | Via di Vigna Murata 605, 00143 Rome, Italy | www.epos-eric.eu

EPOS ERIC

DIGITAL ASSETS MANAGEMENT POLICY

EPOS Digital Assets Management Policy

Status	Public
Written by	EPOS ERIC Policy Working Group: Keith Jeffery, Chris Luton, Lucio Badiali, Daniela Mercurio, Enrico Balli.
Reviewed and Acknowledged by	EPOS ERIC Service Coordination Committee
Date	November 23, 2022
Version	1.0

1. Introduction

The purpose of this policy document is to bring together the separate policies of EPOS for Data and Service providers as well as Users to provide the policy background to ensure that EPOS Data and Services are managed and used in ways that maximise public benefit following FAIR principles (Findability, Accessibility, Interoperability, and Reusability). This policy should be read in conjunction with the EPOS ERIC Statutes (C 2018/7011) and EPOS Data Policy.
Guidelines are also being produced to provide guidance to users and data/service providers on best practice to comply with the policies.
EPOS's mission is to establish and underpin sustainable and long-term access to solid Earth science data and services integrating diverse European Research Infrastructures under a common federated framework. By improving and facilitating the integration, access, use, and re-use of solid Earth science data, data products, services, and facilities, EPOS aims at transforming the European research landscape, driving discovery, and developing solutions to geo-related challenges facing European society.

2. Policy applicability

These policies apply to digital assets providers as well as users who utilise EPOS digital assets.

3. Policy references

The policies are regularly updated in line with any changes in response to the evolution of the EPOS organisational and strategic assets. Any queries or suggestions relating to this policy should be sent to management@epos-eric.eu.

4. Definitions

Terms and phrases in this policy shall have the meanings ascribed to them below.

Digital assets	means a resource with economic or social value that an individual, corporation, or country owns or controls with the expectation that it will provide a future benefit. Digital assets are reported on a company's balance sheet and are bought or created to increase a firm's value or benefit the firm's operations.
Data and Services	mean data, data products, services and software as well as any other technical services supporting the provision of "Data and Services". Data and services are digital assets.
Data and Service Provider	means the organisation in charge of providing "Data and Services".
Data Supplier	means entities granting rights of redistribution of their DDSS through EPOS by signing a Supplier Letter with Data and Service Providers.
DDSS	means Data, Data Products, Services and Software.
EPOS	means the European Plate Observing System Research Infrastructure as defined by Statute.
EPOS Data Portal	means the Integrated Core Services Central Hub (ICS-C).
EPOS Delivery Framework	means the EPOS framework where the relationships among the key actors are regulated by specific rules and procedures. It includes the EPOS ERIC legal seat (represented by the ECO), the Integrated Core Services (ICS) and Integrated Core Services Central Hub (ICS-C) and the Thematic Core Services (TCS).
GDPR	means the General Data Protection Regulation (EU) 2016/679.
General Assembly	means EPOS ERIC General Assembly.
Metadata	means data describing in digital form EPOS digital assets
Statutes	means the Statutes of EPOS ERIC.
TCS	means EPOS Thematic Core Services
Users	means individual or institution that utilises the EPOS Services to access Data and Data Products and/or Tools and Software. Access includes discovery, download, execution, or any other use.

6. Provenance

The provenance policy aims to ensure the record of the life history of digital assets in the EPOS Delivery Framework. Any operation that is carried out on an digital assets has to be recorded (a) for audit; (b) to provide information upon which an end-user can judge the suitability and quality of the digital assets for their purpose; (c) to encourage re-use and reproducibility.
All providers of EPOS digital assets (digital assets suppliers within the TCS and the ICS-C system) shall ensure the availability of the life history of an digital assets by providing appropriate provenance procedures to track and document the life history of an digital assets.

7. Identifier

The identifiers policy is intended to align with the FAIR principles[1]: persistent unique identifiers allow reference to, and direct access to, digital assets[2].
All providers of EPOS digital assets (digital assets suppliers within the TCS and the ICS-C system) shall ensure a universally unique, resolvable persistent identifier for each digital assets at the appropriate level of granularity. Furthermore, since digital assets may have more than one (usually role-based) identifier, identifiers should be federated so that the digital assets can be accessed or referenced by any of the identifiers for the appropriate purpose. Wherever possible, existing standards for identifiers should be followed. The policy is realised by providing appropriate procedures to assign a persistent universally unique identifier to an digital assets. It relates also to the EPOS Data Policy.

8. Quality assurance

The quality assurance policy is intended to guarantee that all users of EPOS shall be assured of the quality of the data and software provided. EPOS ERIC and Data and Services Provider are responsible to assess the quality of data, products, services, and software.
Quality control of the data, products, services, and software rests with the Supplier. Service Providers are responsible for checking the quality parameters of the metadata descriptions that provide information for discovery, contextualization, and provenance and traceability. It relates also to the EPOS Data Policy.
EPOS will disseminate good practice and shall provide a mechanism to obtain User feedback on DDSS quality. EPOS will ensure a continuous process of review and assessment to verify that EPOS DDSS provision is operating as envisioned, seeking improvements and preventing/eradicating problems. EPOS will give emphasis monitoring the quality of the services provided (e.g. response time, number of successful requests). External audit on quality assurance and quality control is also foreseen through an External Scientific Advisory Board.

9. Metadata

The metadata policy aims to align with the FAIR principles: metadata provides the information to utilise digital assets.
All providers of EPOS digital assets (digital assets suppliers within the TCS and the ICS-C system) shall ensure rich metadata describing each digital assets at the appropriate level of granularity. Rich metadata is metadata sufficient for the purpose of discovery, contextualization (relevance/quality), access (appropriate information to control access including licensing), and (re-)use (including any changeable parameters to control the digital assets). The metadata must be

[1] https://www.force11.org/group/fairgroup/fairprinciples
[2] https://en.wikipedia.org/wiki/Digital_digital assets

in the current EPOS standard for the metadata catalog (CERIF[3]) to be recognized as a digital asset within the EPOS Delivery Framework.
The policy is realised by providing appropriate procedures to assign rich metadata to a digital asset. It relates also to the pre-existing EPOS Data Policy.

10. Licensing

The EPOS licensing policy will facilitate effective rights/ownership management over redistribution of Data, Data Products, Software and Services (DDSS) acquired/created by EPOS. EPOS shall only redistribute DDSS to which an appropriate licence has been applied/affixed (EPOS Data Policy). EPOS aims to grant one default licence set for EPOS-managed DDSS, namely the Creative Commons 4.0. licence (CC:BY or CC:BY:NC). In exceptional cases where a licence cannot be applied, the Service Providers shall inform EPOS ERIC.
EPOS recognises that it is essential that metadata for DDSS are easily and freely accessible at any time, with as few restrictions as possible, to ensure the widest dissemination and publicity for EPOS managed DDSS. In order to achieve this, Digital Asset Suppliers shall affix open licences, preferably Creative Commons 4.0 CC:BY, to their metadata. The licence applied will place obligations on users of the digital asset, such as acknowledgement where appropriate information is provided.
Software will be treated differently to other EPOS managed DDSS and licensed under a software licence in common usage. Software made available as digital assets by Digital Asset Suppliers shall have affixed an appropriate software licence. The licence applied will place obligations on users of the software digital asset such as acknowledgement and possibly constraining software developed from that supplied to utilise the same licence. It is recommended to use GPLv3 for Academic purposes (protecting open use) and Apache2 for business purposes (protection of intellectual property). In the case of the EPOS data portal and associated systems, GPLv3 shall be used unless specific components (e.g., an API) are to be developed in a commercial environment in which case Apache2 shall be used.

11. Security/Authentication

The security/authentication policy aims to define the governance of persons accessing or providing EPOS digital assets within the EPOS Delivery Framework (EDF) and to record their usage of digital assets if/when required. In particular, authentication ensures that a person is who they claim to be. It is part of the security policy, the other parts being authorization, physical security, and disaster recovery.
All users and suppliers of EPOS digital assets shall be authenticated at the appropriate stage of access. EPOS will implement appropriate authentication wherever required either from a supplier or user perspective. EPOS will use any information about users gained through authentication mechanisms according to the privacy policy.

[3] https://eurocris.org/services/main-features-cerif

The policy is implemented by a check of a person's identity with respect to EPOS declared by a responsible person. The implementation requires that mechanisms are in place to allow users to authenticate themselves using EPOS approved Identity Providers (IdPs). (the approved IdPs are listed in the guidelines).
The implementation (guidelines) includes checking that the user is not barred from accessing EPOS due to any legal restrictions.

12. Security/Authorisation

The security/authorisation policy aims to define the governance of persons supplying or accessing EPOS digital assets within the EPOS Delivery Framework (EDF). In particular, authorisation defines the digital assets (or digital assets classes) a person may access, in what role (e.g. user, manager), in what modality (**C**reate; **R**ead; **U**pdate; **D**elete; **E**xecute; down**L**oad) and within what time period. Authorisation balances the rights of the user (such as open access) against the rights associated with the digital assets (such as a licence). A prerequisite is user authentication. It is part of the security policy, the other parts being authentication, physical security and disaster recovery.
All users of EPOS digital assets must be authorised to access digital assets in the appropriate role, modality, time period either explicitly (permissions linked to authenticated identity) or by default (where the digital assets is not so protected). The latter is so-called anonymous use, although the user identity (authentication) and relevant attributes may be utilised for recording usage.
The policy is implemented by a record of a person's rights to access EPOS digital assets in the appropriate role, modality, time period declared by a responsible person.
The implementation requires that, for any EPOS digital assets that requires authorisation a process exists for a defined, authorised person to declare that a given user has a right to access a specific EPOS digital assets in the appropriate role, modality, time period, and that the person (user) is registered at a node of the EPOS delivery framework with appropriate details in the associated Identify Provider (IdP).

13. Curation

The curation policy aims to define the lifecycle management of digital assets in the EPOS Delivery Framework.
All providers of EPOS digital assets (digital assets suppliers within the TCS and the ICS-C system) must ensure: a) availability of the digital assets (whether DDSS or metadata) and b) the integrity and availability of the digital assets (subject to security, authentication, authorisation policies). Digital assets quality is dealt with in the quality assurance policy.
The policy is realised by (a) deciding whether a digital assets should be curated or deleted; in the latter case a "tombstone" metadata record should be available; (b) provision of appropriate backup and replication procedures sufficient to recover digital assets should there be unavailability or corruption due to e.g., a security breach or power failure.

14. Disaster Recovery

The disaster recovery policy aims to ensure that IT resource investments made by EPOS are protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of disaster recovery plans.
This policy applies to all facilities of EPOS that operate, manage or use IT services or equipment to support mission-critical functions.
IT resource investments made by EPOS shall be protected against service interruptions, including large-scale disasters, by the development, implementation, and testing of disaster recovery plans. In particular, the following actions plans and actions be implemented:

- plans for disaster recovery shall be developed by IT management;
- disaster recovery plans shall be updated at least annually and following any significant changes to the computing or telecommunications environment of EPOS;
- IT staff of EPOS shall be trained to execute the disaster recovery plan;
- annual testing of the disaster recovery plan shall be done;
- an external auditor shall audit disaster recovery plans.

15. Physical security

The Physical Security Policy aims to protect and preserve information, physical digital assets, and human digital assets. Thus, EPOS information, physical digital assets, and human digital assets shall be protected and preserved:

- physical access to the server rooms/areas shall completely be controlled and servers shall be kept in the server racks under lock and key;
- access to the servers shall be restricted only to designated Systems and Operations Personnel;
- besides them, if any other person wants to work on the servers from the development area then he/she shall be able to connect to the servers only through Remote Desktop Connection with a Restricted User Account;
- critical backup media shall be kept in a fireproof off-site location in a vault.

All facilities of EPOS that operate, manage, or use IT services or equipment to support mission critical functions shall:

- establish the rules for granting, control, monitoring, and removal of physical access to office premises;
- identify sensitive areas within the organisation;
- to define and restrict access to the same.

16. Terms and Conditions

The Terms and Conditions aims to govern the contractual relationship between EPOS and its users of the sites https://www.epos-eu.org and https://www.epos-eu.org/dataportal. The relationships between EPOS ERIC and Data and Service Providers for the purposes of provision are additionally subject to separate agreements.

Full Terms and Conditions are available at: https://www.epos-eu.org/sites/default/files/Terms_and_Conditions.pdf

17. Cookies

The Cookies Policy aims to describe how the site https://www.epos-eu.org uses cookies and processes personal data of users who visit it. In compliance with the obligations arising from national and EU legislation (EU Regulation 679/2016) and subsequent amendments, this Site respects and protects the privacy of visitors and Users, making every possible and proportionate effort not to infringe their rights. This cookie policy applies only to the online activities of this Site and is valid for visitors/Users of the Site. It does not apply to information collected through channels other than this Website. The purpose of the policy is to provide maximum transparency regarding what information the Site collects and how it uses it. EPOS-ERIC ICS-C portal https://www.epos-eu.org/dataportal uses cookies only to monitor performance anonymously, information used in improving the portal. You may choose to allow these cookies or not. Either choice does not prevent use of the portal.
Full Cookies policy is available at:
https://www.epos-eu.org/sites/default/files/Cookie_Policy.pdf

18. Privacy

The Privacy Policy aims to give information on how EPOS collects and processes personal data, through the use of the site www.epos-eu.org or when subscribed to EPOS services or otherwise engaged with any of EPOS projects or applying for a position with EPOS. In compliance with the obligations arising from national and EU legislation (EU Regulation 679/2016) and subsequent amendments, this Site respects and protects the privacy of visitors and Users, making every possible and proportionate effort not to infringe their rights.
Full privacy policy is available at: https://www.epos-eu.org/epos-eric-privacy-policy

19. Attribution, Acknowledgement, Citation

The Attribution, Acknowledgement, Citation Policy aims to: i. ensure that appropriate Attribution, Acknowledgement, Citation information is included with any data or service provided to a user; ii. support efforts to improve Attribution, Acknowledgement, Citation of original (digital assets) providers/suppliers in scientific publications and during the whole research data life-cycle.
Generally, within global research and academic fields, an acknowledgement is a declaration or avowal of one's own act, often used to acknowledge ownership, supply or provision, thereby giving the DDSS legal validity, and works to prevent the recording of false or fraudulent claims. Creative Commons licences utilising the “BY” element will require acknowledgement to be given to the Supplier. Both acknowledgement and citation rely on attribution: the association of the digital assets with a person or organisation that created (directly or by assembling, curating), and has ownership or delegated stewardship, of the digital assets.

All DDSS supplied by EPOS will be provided by licence. One of the obligations of a licensee will be to acknowledge or cite the source of the digital assets (where known).
Owners, Suppliers or Providers may well be requested by EPOS to provide details of how they wish to be acknowledged, and users will be legally bound to match those requirements. This is usually defined by the licence.
This policy applies to all owners, suppliers, providers and users of EPOS DDSS.