ESA ESRIN
Largo Galileo Galilei 1
00044 Frascati
Italy

END-USERS ACCESS POLICY TO ESA AND THIRD PARTY MISSION DATA, TOOLS AND RESOURCES

APPROVAL

Title	END-USERS ACCESS POLICY TO ESA AND THIRD PARTY MISSION DATA, TOOLS AND RESOURCES		
Issue Number	1	Revision Number	0
Author	EOP-GES	Date	24/07/2024
Approved By	Francesca Cipollini	Date of Approval	09/09/2024

CHANGE LOG

Reason for change	Issue Nr	Revision Number	Date

CHANGE RECORD

Issue Number	Revision Number		
Reason for change	Date	Pages	Paragraph(s)

DISTRIBUTION

Name/Organisational Unit

Table of Contents

1. INTRODUCTION

1.1. Purpose and Objectives

The purpose of this policy is to establish a framework for determining user access to resources provided by Ground Segment and Data Management Division (EOP-GE) including functions and data based on assigned user attributes and types.

1.2. Scope

The policy is directed at End Users which are a category defined in EO GS User Classification document [RD-1].

Through the implementation of this policy, End User access will be automatically managed based on their privileges, thereby minimizing the necessity for manual intervention.

The following EOP-GE functional areas [AD-4] have been identified as relevant to End Users:

- **Data Access** provides users with the ability to access and retrieve data from various sources.
- **User Help Desk** provides users with assistance and support for any issues or questions they may have. It can include a variety of support options such as phone, email, or chat support, and may also provide access to resources such as FAQs or user guides.
- **User Experience Benchmarking** involves evaluating and measuring the user experience of a product or service. It can include collecting feedback from users, conducting user testing, and analyzing data to identify areas for improvement and optimize the user experience.
- **User Management** allows users to manage their own accounts and preferences. It can include features such as authentication and authorization mechanisms to ensure that users only have access to the data they are authorized to view, the ability to update personal information, change passwords, and manage privacy settings.

- **User Collaborative Environment** provides users with a virtual environment for collaboration.
- **User Communication & Information Portal:** Information Portal represents the primary informative interface with Users Community. It is in charge of presenting available satellite missions, EO products, additional information and documentation concerned with satellite instruments. IFP provides the required knowledge to help the Users Community in a quick identification of products/data of interest.
- **Processor Development & Maintenance** includes maintaining and updating algorithms used in a product or service. It can include tasks such as fixing bugs, optimizing performance, and adding new features or capabilities.
- **Calibration & Validation** service involves the usage of calibration and validation tools to perform calibration and validation activities on data by the dedicated community.

1.3. Policy Ownership

This policy is owned by the EOP-GE division, which is responsible for defining, maintaining, and updating the policy as per the business needs and regulatory requirements. The policy owner also ensures that the policy is communicated and disseminated to all relevant stakeholders and that the policy objectives are met and monitored.

1.4. Applicable and Reference Documents

ID	Document Reference	Document Title	Link
[AD-1]	ESA-EOPG-PDGS-PR-1	Terms and Conditions for the Utilisation of ESA's Earth Observation Data between the EUROPEAN SPACE AGENCY and the Principal Investigator	T&C for the Utilisation of Data

[AD-2]	ESA/PB-EO(2010)54	EUROPEAN SPACE AGENCY EARTH OBSERVATION PROGRAMME BOARD Revised ESA Data Policy for ERS, Envisat and Earth Explorers missions	EO Data Policy
[AD-3]	ESA-EOPG-PDGS-PR-2	Terms and Conditions for the Utilisation of Data under ESA's Third Party Missions scheme between the EUROPEAN SPACE AGENCY and the Principal Investigator	T&C for the Utilisation of Data
[AD-4]	ESA-EOPG-PDGS-DD-2024-4	EO EOF-EOS Functional Analysis	N/A

Table 1: Applicable Documents

ID	Document Reference	Document Title	Link
[RD-1]	GMGT-SENE-EOPG-10-0007	EO PDGS User classification	N/A
[RD-2]	N/A	European Space Agency Personal Data Protection Framework	European Space Agency Personal Data Protection Framework
[RD-3]	ESA Security Directives	ESA-ADMIN-IPOL-SEC(2020)1_FINAL_EN	N/A
[RD-4]	GMGT-SENE-EOPG-PD-10-0004	EO PDGS Implementation of EO Network Security Policy	N/A

[RD-5]	GMGT-SECR-EOPG-PD-07-0001	ESA Earth Observation Ground Segment Security Policy	N/A
[RD-6]	ESA-EOPG-PDGS-ML-2024-1	PDGS COMMON GLOSSARY	N/A
[RD-7]	N/A	Access to COSMO-Skymed as ESA's Third Party mission	COSMO-Skymed Terms of Applicability
[RD-8]	N/A	Access to GHGSat as ESA's Third Party Mission	GHGSat Terms of Applicability
[RD-9]	N/A	Access to SPOT, Pleiades and Pléiades-Neo as ESA's Third Party Mission	SPOT, Pleiades and Pleiades-Neo Terms of Applicability
[RD-10]	N/A	Access to ICEYE as ESA's Third Party mission	ICEYE Terms of Applicability
[RD-11]	N/A	Access to GEOSAT-1 & -2 as ESA's Third Party Mission	GEOSAT 1&2 Terms of Applicability
[RD-12]	N/A	Access to NovaSAR-1 as ESA's Third Party Mission	NovaSAR-1 Terms of Applicability

[RD-13]	N/A	Access to PAZ as ESA's Third Party mission	PAZ Terms of Applicability
[RD-14]	N/A	Access to Indian data as ESA's Third Party Mission (IRS-1C/1D, Resourcesat-1/2, Cartosat-1) through GAF AG	Access to Indian Data Terms of Applicability
[RD-15]	N/A	Access to ESA's Planet Missions	Planet Missions Terms of Applicability
[RD-16]	N/A	Access to RADARSAT data as a TPM	RADARSAT Terms of Applicability
[RD-17]	N/A	Access to SPIRE as ESA's Third Party mission	SPIRE Terms of Applicability
[RD-18]	N/A	Access to TerraSAR-X/TanDEM-X as ESA's Third Party Mission	TerraSAR-X/TanDEM-X Terms of Applicability
[RD-19]	N/A	Access to Vision-1 as ESA's Third Party Mission	Vision-1 Terms of Applicability
[RD-20]	N/A	Access to WorldView, GeoEye-1, QuickBird as ESA's Third Party Mission –	WorldView, GeoEye-1 & Quickbird Terms of Applicability

[RD-21]	Governance Framework	Governance Framework	
[RD-22]	N/A	Earth Observation Identity Access Management System (EO-IAM) Privacy Notice	Privacy Notice

Table 2: Reference Documents

1.5. Acronyms

MM	Mission Management
PI	Principal Investigator
ESA PDP	ESA Personal Data Protection Policy
EOP-G	Earth Observation Department – Ground Segment
GS	Ground Segment
PDGS	Payload Data Ground Segment
EOP-GE	Ground Segment and Data Management Division
EO	Earth Observation

For more information, please consult the PDGS Common Glossary [RD-6]

1.6. Definitions

Authentication:

Authentication

Is the process of confirming the correctness of the claimed user identity.

Authorization

Authorization is the process of granting or not access to a protected resource to a user, based on information available about such a user.

Identity Federation

Identity Federation is a group of institutions that agreed about policies for exchanging information about their users in order to grant access and utilization of protected resources and services.

Access Conditions

Access conditions refer to a category of authorisation information that specifies the requirements or criteria that a user must meet in order to access a resource or service. Access conditions can be based on user attributes, such as group membership, role, assurance level, or affiliation, or on other factors, such as time, location, device, or IP address. Access conditions are usually defined by the resource owner or administrator and enforced by the proxy or the end service.

User category

User category refers to a classification of users based on their roles, attributes, and needs. A user category defines the level of access and service that a user is entitled to receive from the Ground Segment. User categories are assigned by the Ground Segment administrator according to the EO PDGS User Classification document [RD-1]. A user category can have many types, as per Table 4. Each type of user category has different privileges and responsibilities.

User Type

A user type is a specific role that a user can have within a user category, based on their tasks, available tools and expertise. For example, a standard user is a user type in the End User category.

Level of Trust

Level of Trust is a classification of users based on the attributes that each user possesses. All End Users who interact with ESA EO functions are assigned a Level of Trust. The classification of the established Level of Trust as defined by this policy can be found in Table 3.

2. USER MANAGEMENT

As mentioned previously End Users are the target category of this policy. End Users have expertise in their own scientific domain. They are not familiar with the functions outlined in section 1.2. They must be able, as much as possible, to perform their tasks unassisted using the available interfaces. There are several types of End Users, as outlined in Section 2.2.

2.1. Classification of ESA systems users

All End Users who interact with ESA EO functions are assigned a Level of Trust.
The classification of the established Level of Trust as defined by this policy can be found in the table below.

Level of Trust		Definition
Unverified	**Unauthenticated**	Users that access the service as guests, without finalizing the registration. They have limited access and are typically restricted to public information or basic functionalities. This role may be granted by default to users who have not yet created an account or logged in.
Verified	**Authenticated**	Users who have created an account and logged into the system. They have established a basic level of trust. Registered users may have access to additional features and personalized settings. Registered Users have registered in the GS system and thus have a user profile. They can be any private individual or part of an organisation/company and there are no prerequisite to registration other than the mandatory registration fields.
	Authorized	Users who have gone through an additional verification process to establish a higher level of trust. This verification may involve confirming their identity,

		providing additional information, or undergoing a background check. Users with institutional/company account of an institution/company that collaborates or has collaborated in the past with ESA (e.g.: university and industrial partners).

Table 3: ESA Systems User Types

It is worth nothing that the Level of Trust is not fixed for and End User and can change. In order to increase their Level of Trust, End Users must be subjected to a verification process which can include identity, affiliation and eligibility checks. Increased Levels of Trust may grant the user access to more functions such as restrained data.

2.2. End User Types

The section outlines the types of End Users as defined by the policy, with corresponding access conditions and available functions. End User types are sub-categories of the End Users category. A user can belong to multiple user categories however can only be assigned one End User Type (anonymous users do not have a profile and therefore are excluded from this assumption).

Table 4: End User Types

User Type	Definition	Access Conditions	Functions*[1]	Level of trust*[2]	Notes
Anonymous User	An Anonymous User is a user accessing a function, however, is not (yet) registered or has not signed in.	Not Applicable	• User Communication & Information Portal • User experience benchmarking[a] • User Management[b] • Data Access[c] • User Help Desk[d]	**Unverified-unauthenticated**	[a]Partial access to public web user satisfaction forms and surveys at events [b] only registration functionalities [c] to be intended as data discovery here [d] Simple request form only for helpdesk access
Standard User	A Standard User has registered via the identity and access management entry point and thus has a user profile with automatically assigned standard privileges.	Registration/Federation Acceptance of T&C Country of Residence	• User Communication & Information Portal • User experience benchmarking • User management • Data access [a] • User Help Desk [b]	**Verified-Authenticated**	[a] access to open data only [b] full standard user helpdesk without advanced user helpdesk
Advanced User	An Advanced User has requested access to additional functions and has	Registration/Federation Acceptance of T&C Country of residence Referral by GSM	• User Communication & Information Portal • User experience benchmarking	**Verified – Authorized**	[a] access to restrained data for which the user has the applied data access condition

User Type	Definition	Access Conditions	Functions*[1]	Level of trust*[2]	Notes
	been granted the privilege to access them. To grant these privileges a manual check is performed, and authorization is given.	Work email address	• User management • Data access [a] • User Help Desk • User Collaborative Environment		
Cal/Val Users	A Cal Val User is an expert PI responsible for providing feedback on cal/val activities. These users are elevated upon request and approval by MM or Project Team	Registration/Federation Acceptance of T&C Country of residence Referral by MM/Project Team	• User Communication & Information Portal • User experience benchmarking • User management • Data access [a] • User Help Desk • User Collaborative Environment • Processor Development and Maintenance • Cal/Val	**Verified - Authorized**	[a] access to restrained data for which the user has the applied data access condition

User Type	Definition	Access Conditions	Functions$*^{1}$	Level of trust$*^{2}$	Notes
Mission Team	These users belong to a team responsible for development, commissioning & operational phase of the mission. Includes MM and GSM, Project Team, Operations Team, Satellite prime and Instruments prime and industrial partners	Registration/ Federation Acceptance of T&C Being a recognized member of this team	• User Communication & Information Portal • User experience benchmarking • User management • Data access • User Help Desk • User Collaborative Environment • Processor Development and Maintenance • Cal/Val	**Verified – Authorized ESA verified**	

$*^{1}$ The logic for granting functions access is cumulative, meaning that each user type inherits the functions access from the previous user type in the same category, plus some additional functions specific to that user type

$*^{2}$ For further information, please refer to Table 3.

2.3. Implementation

Each function is responsible for developing and executing its own implementation strategy in alignment with this policy. This ensures that specific requirements of each function are appropriately addressed, promoting effective and efficient resource management.

2.4. User Account Maintenance

The account maintenance is performed in accordance with the Privacy Notice of the Identity and Access Management entry point [RD-22] which informs the users about their rights and obligations regarding their personal data. The privacy notice also specifies how users can request access, correction, deletion, or restriction of their data, as well as how they can withdraw their consent or lodge a complaint. The account maintenance aims to protect the users' privacy and security, as well as the integrity and functionality of the system.

The system will automatically anonymize End-User accounts that have been inactive (no login or account interaction) for more than 24 calendar months. The End-User will be notified prior to the anonymization and will be given the opportunity to reactivate their account. End-User account anonymizations are performed to ensure compliance the European Space Agency Personal Data Protection Framework [RD-2].

3. FEDERATED USERS ACCESS

Different organisations have internal mechanisms for providing users with digital identities. Nevertheless, each organisation providing EO Data and related functions is expected to put in place some rules that represent the basis for the Federated single sign on use case that will allow distributed and simplified access to the data.

The policy covers users managed by federation with other entities. Federated users are standard users (e.g. Academia or National Space Agencies) and they need to request authorization to access more privileges. The same logic shall apply to ESA Federated users.

4. USER REPONSIBILITIES AND ACCEPTABLE USAGE

4.1. Responsibilities

The responsibilities of users with regards to access and usage of the functions, include but are not limited to:

- compliance with any security protocols in [RD-3]
- usage of resource only for the purpose specified
- compliance with established controls and rules [RD-5]
- reporting any suspected security breaches and incidents or any inconsistencies via the following form link
- acknowledgement of the source of the data
- installation of strictly permitted software as indicated in the User Manual of the system
- protection of own credentials
- entry of systems only when and if authorized
- avoiding excessive consumption of resources
- providing true and accurate information if and when requested to do so
- creation of single user accounts (multiple accounts shall not be created by one user unless explicitly agreed with ESA)

4.2. Acceptable Usage

Users should agree to use the functions in a responsible and ethical manner, respecting the rights and interests of other users and third parties. They will not use the functions for any illegal, harmful, fraudulent, or offensive purposes, or to transmit, store, or distribute any content that violates the rights of others. They shall not interfere with or disrupt the operation of the functions or the access of other users.

4.3. Copyright, Restrictions and Permissions Notice

ESA retains all rights and title over the ESA EO systems and data [AD-2] facilitated via the functions in section 1.2.

ESA's title and copyright of the systems shall not prevent recognition of copyright in favour of an End User which may arise as a result of the latter's own interpretation of an ESA system created or processed data, algorithm, input of data or knowledge from other sources.

Users shall not use any data or systems provided by ESA in any manner that infringes or violates the intellectual property rights of ESA or its data providers and partners, or that misrepresents or damages their reputation or goodwill.

Users shall cite and reference the source of any systems obtained from ESA in any publications, presentations, reports, or other outputs that make use of them, following the citation guidelines provided by ESA or its data providers and partners. Users shall also provide feedback to ESA on the quality, usability, and impact of the systems, as well as on any issues or errors encountered while using them.

Users shall cooperate with ESA in any audits, investigations, or inquiries related to the use of the data and systems and shall promptly notify ESA of any actual or suspected breach.

4.4. Algorithms derived from systems released by ESA under Creative Commons Attribution-ShareAlike 3.0 IGO (CC BY- SA 3.0 IGO) Licence

Where expressly so stated, algorithms are covered by the Creative Commons Attribution-ShareAlike 3.0 IGO (CC BY-SA 3.0 IGO) licence, ESA being an Intergovernmental Organisation (IGO), as defined by the CC BY-SA 3.0 IGO licence.

The terms used with capitals herein are defined in the CC BY-SA 3.0 IGO licence.

The user is allowed under the terms and conditions of the CC BY-SA 3.0 IGO licence to Reproduce, Distribute and Publicly Perform the ESA algorithms released under CC BY-SA 3.0 IGO licence and the Adaptations thereof, without further explicit permission being necessary, for as long as the user complies with the conditions and restrictions set forth in the CC BY-SA 3.0 IGO licence, these including that:

The source of the algorithm is duly credited (Examples: “Credit: ESA/Rosetta/NavCam – CC BY-SA IGO 3.0”, “ESA/DLR/FU Berlin, CC BY-SA 3.0 IGO”, CC BY-SA 3.0 IGO”), and a direct link to the CC BY-SA 3.0 IGO licence text is provided.
No warranties are given. The licence may not give the user all of the permissions necessary for the intended use. For example, other rights such as publicity, privacy, or moral rights may limit how the user uses the material.
To view a copy of this license, please visit http://creativecommons.org/licenses/by-sa/3.0/igo/.

5. GOVERNANCE

EOP-GE will define a governance framework to ensure that the policy is adhered to by all End Users and service providers. The framework will set out the procedures and mechanisms for monitoring, reporting, and resolving any issues or conflicts that may arise from the implementation of the policy.
Furthermore, a feedback mechanism shall be implemented to allow for reporting of issues or suggestions for improvement, ensuring the policy remains relevant and effective.

6. PRIVACY, DATA PROTECTION AND SECURITY

The policy shall ensure that the privacy and data protection rights of its users are respected, and it shall further ensure the security of the information shared on the platform.

The policy shall align with the:

- Privacy and data protection will be aligned with the ESA Personal Data Protection Framework [RD-2]
- Security will be ensured according to the EOP-G security framework, [RD-5]

7. POLICY REVIEW AND UPDATE

Unless otherwise required, the policy will be reviewed and updated on an annual basis to reflect any changes in the legal, technical, or operational environment. The policy review and update

process will involve consultations with relevant ESA stakeholders. The revised policy will be communicated to all parties through the website and email notifications as needed.