***PRIVACY NOTICE***

***Introduction***

The European Space Agency (herein the "Agency" or "ESA") is an intergovernmental organisation established by its Convention opened for signature in Paris on 30 May 1975 having its headquarters located in Paris, France.

Protection of Personal Data is of great importance for ESA, which strives to ensure a high level of protection as required by the ESA Framework on Personal Data Protection ("the ESA PDP Framework") which applies in this field. ESA implements appropriate measures to preserve the rights of Data Subjects, to ensure the processing of Personal Data for specified and legitimate purposes, in a not excessive manner, as necessary for the purposes for which the Personal Data were collected or for which they are further processed, in conditions protecting confidentiality, integrity and safety of Personal Data and generally to implement the principles set forth in the PDP Framework, available at: http://www.esa.int/About_Us/Law_at_ESA/Highlights_of_ESA_rules_and_regulations.

The ESA PDP Framework is composed of the following elements:

- the Principles of Personal Data Protection, as adopted by ESA Council Resolution (ESA/C/CCLXVIII/Res.2 (Final)) adopted on 13 June 2017;
- the Rules of Procedure for the Data Protection Supervisory Authority, as adopted by ESA Council Resolution (ESA/C/CCLXVIII/Res.2 (Final)) adopted on 13 June 2017; and
- the Policy on Personal Data Protection adopted by Director General of ESA on 5 February 2018 and effective on 1 March 2018.

This notice is intended to inform you, as a Data Subject, about:

- the identity of the Data Controller and contact details of ESA's Data Protection Officer ("DPO");
- the type of Personal Data which is collected and processed;
- the modalities of collection of Personal Data;
- the purpose of the collection and processing;
- the recipients (if any) to whom the Personal Data of the Data Subject shall be disclosed;
- the time-limits for storing the Personal Data;
- the practical modalities of exercising the rights of the Data Subject under the ESA PDP Framework.

This notice also enables ESA to obtain your consent relating to the collection and further processing of your Personal Data, under the ESA PDP Framework.

### *(1) Who is the Data Controller?*

Your Personal Data are collected and further processed as shown below upon the decision taken by ESA. For this reason, ESA is the Data Controller under the ESA PDP Framework.

### *(2) What are the contact details of ESA's Data Protection Officer?*

Your first point of contact concerning Personal Data matters is ESA's Data Protection Officer ("DPO"), who may be contacted at:

**email:dpo@esa.int**

**tel: +33 1 53 69 72 69.**

### *(3) What kind of Personal Data about you are collected and further processed by EO Sign In?*

The Personal Data, which are collected and further processed for the purposes mentioned below, are in particular:

- Your first name, last name,
- Institution
- Country of residence
- Username (e-mail address)
- Contact email address
- IP (internet protocol) address used to log in
- Your device ID if you use a device (e.g., phone or tablet) to log in
- Your answers to security questions
- Browser fingerprinting
- Current password and previously used passwords
- City/Country from which you originated the TCP/IP connection
- Time of day that you logged in (year, month, week, hour or minute)
- Operating system and generic browser information
- Information retrieved through browser cookies such as the user's IP address, geolocation, date and time of the visit, URL visited.

You are required not to send to the Agency any sensitive information (including information that indicate, directly or indirectly, the personnel's ethnic origin, political opinions, adhesion to unions, parties etc., health situation, sexual orientation).

### *(4) How are your Personal Data collected or further processed?*

Your Personal Data are collected when you register for an EO Sign In account and when you use the services accessed with this account.

EO Sign In collects your Personal Data by:

- Collecting information from the user profile page where you enter your Personal Data.
- Tracking your IP address with HTTP request, HTTP headers, and TCP/IP.
- Tracking your geographic information with the IP address.
- Tracking your login history with browser cookies. Please see our cookie policy for more information.

ESA manages the EO Sign In and data access related services through Contracts. The companies responsible for the contracted services act on ESA's behalf to ensure your Personal Data is protected in accordance with ESA's Personal Data Protection Policy and European Union Personal Data protection standards.

Under ESA's contract with Serco, your Personal Data will be processed by the ESA EO Helpdesk, on behalf of ESA, to provide access to ESA EO Data by associating the proper access rights to your account.

ESA and its contractors will not use your Personal Data for any purpose other than supporting the services connected to the EO Sign In and will not disclose your Personal Data to any other entity that is not listed under (7). They do not consider your Personal Data as an asset for sale and will not sell your Personal Data to any third parties.

## *(5) Where is your Personal Data stored*

The servers of ESA are located in data centres hosted by ESA in ESRIN, Frascati, Italy and operated by *GTT Communications, Inc* (GTT) and accessed by *Serco Italia S.p.A*. (Serco).

## *(6) Why are your Personal Data collected and further processed?*

Your Personal Data are collected and further processed for the following purposes:

- to provide you access to ESA's Earth Observation (EO) data and EO data from Third-Party Missions: EO Sign In requires a personal profile (username, first name, last name, email address, institution, country of residence and contact email) to authenticate the log in and allow access to the requested data, based on set access rights;
  In that respect, EO Sign In discloses Personal Data to the relevant applications (also known as Service Providers) that are registered with EO Sign In and registered by the ESA identity administrator. Personal Data is disclosed only for the purpose of providing the users with ESA EO Data Access and User Support services (or for a use identified as consistent with that purpose), as controlled by such Service Providers, unless you have consented otherwise or where law requires it.

- to communicate with you if you submit an enquiry (contact email address);
- if required, to communicate your Personal Data (last name, first name, email address, institution, country of residence) to third party data providers to obtain their agreement to the specific data access request;
- to generate statistics about the activity of ESA's EO data users (e.g. log-in behaviour, type and volume of EO data downloaded, most frequently requested data, etc). Please note that the statistics themselves are aggregated and anonymised and do not contain any Personal Data;
- For security purposes: EO Sign In processes your IP address and browser fingerprinting to protect your account from unauthorized access or potential hacking and uses your security questions and answers only to allow account recovery.

In addition to these purposes, the Agency may use your Personal Data for any of the purposes mentioned in Article 5 of the Policy on Personal Data Protection.

### *(7)To whom might we disclose your Personal Data?*

The Agency may disclose your Personal Data to any of the following third-party recipients for the fulfilment of all or part of the purposes of the collection and processing of Personal Data which are mentioned above:

- *ServiceNow Nederland BV* (ServiceNow) and *Highmetric LLC* (Highmetric), Airbus Defence and Space, Eversis Sp. Z.o.o and Progressive Systems srl, all under contract with ESA. The servers are located at their sites in ESA Member States (Italy, The Netherlands, United Kingdom and Poland).
- VTT (https://www.vttresearch.com/en/data-privacy-and-accessibility), Vista (https://www.vista-geo.de/en/privacy-policy/) and Terradue for the access to the relevant Thematic Exploitation Platforms.
- Third-Party data providers, who are the owners of the Third-Party EO data distributed by ESA and need separately to authorise access to their data:
    - Airbus Defence and Space for access to TerraSAR-X, Pleiades and SPOT data (https://www.airbus.com/privacy-policy.html)
    - BELSPO for access to PROBA-V data (https://www.belspo.be/belspo/organisation/privacy_en.stm)
    - Deimos Imaging for access to Deimos-1 and Deimos-2 data (https://www.deimos-imaging.com/privacy-policy/)
    - European Space Imaging, for access to GeoEye, Quickbird, WorldView-1/2/3 data (https://www.euspaceimaging.com/privacy-policy/)
    - e-GEOS for access to Cosmo-Skymed data (https://www.e-geos.it/#/privacy)
    - GAF AG for access to Resourcesat-1, Resourcesat-2, Cartosat-1 and IRS-1C/1D data (https://www.gaf.de/?q=content/privacy-policy)
    - Hisdesat for access to PAZ data (https://www.hisdesat.es/en/legal#cookies)

- ICEYE for access to ICEYE data (https://www.iceye.com/privacy-policy)
- MacDonald Dettwiler for access to Radarsat-1 and Radarsat-2 data (https://mdacorporation.com/corporate/privacy-policy/)
- Planet for access to Rapideye, Planetscope and SkySat data (https://www.planet.com/privacy/)
- Spire for access to Spire data (https://spire.com/privacy-policy/)
- Remote Sensing Applications Consultants Ltd for access to Proba-1 data
- Surrey Satellite Technology Ltd for access to Proba-1 data (https://www.sstl.co.uk/privacy-policy).

ESA draws your attention to the fact that if you make a request for Third-Party data listed above, your Personal Data (e.g. last name, first name, email address, institution, country of residence) may be processed in a country which is not a member state of ESA and/or the European Union and which is not recognised by the European Commission as offering an adequate level of protection under the European Union's legal framework.

### *(8) How long do we retain your Personal Data for?*

The Agency and its contractors may keep your Personal Data for as long as necessary for the fulfilment of the above-mentioned purposes. Your Personal Data shall be deleted thereafter.

If you do not confirm your registration to the EO Sign In when you are sent the confirmation link by email, your Personal Data will be automatically deleted from all servers within 60 days of the initial account creation request.

If you do confirm your registration to the EO Sign In, your Personal Data will be stored on the ESA and third parties servers for as long as you are an active user of the EO Sign In service.

Your Personal Data will be deleted after two years of inactivity, prior notification by email of account being locked, unless you confirm you wish the account to remain open.

### *(9) How can you erase, rectify, complete or amend your Personal Data?*

The Agency is keen to collect and process only accurate Personal Data and to keep it up-to-date.

Under ESA's Personal Data Protection Framework, you have the rights, which you may exercise at any time, to have your Personal Data erased, rectified, completed or amended. You are able to access your Personal Data and rectify, complete or amend the information contained in your account profile autonomously after log in into EO Sign In using your personal dashboard. For the deletion of your account, please contact the ESA EO Front-End Services Helpdesk.

If you choose to erase your Personal Data or do not accept the terms of this Privacy Notice, you understand and agree that ESA will have to delete your ESA EO Sign In account and you will lose all of your rights for accessing ESA's EO data and services through your ESA single sign-on account.

If you are unable to access your account for any reason or need support, please contact the ESA EO Front-End Services Helpdesk for assistance.

### *(10) What could you do in the event of a Data Protection Incident?*

In the event of a Data Protection Incident, please contact ESA's DPO, as the first point of contact, by sending an email to dpo@esa.int.

If you wish to submit a complaint, you will need to comply with the Rules of Procedure of the Supervisory Authority set out in the ESA PDP Framework. You will be required to demonstrate that a Data Protection Incident occurred in relation to your Personal Data, following a decision of the Agency, or at least to justify serious reasons to believe that such an incident occurred.