



# EnMAP

## ENMAP SERVICES DATA PROTECTION DECLARATION

---

For the automated processing of personal data as part of providing the Services of EnMAP

## EnMAP Services Data Protection Declaration

The German Aerospace Center (Deutsches Zentrum für Luft- und Raumfahrt e. V., hereinafter referred to as "DLR") takes the protection of personal data very seriously. We want you to know when we store data, which types of data are stored and how it is used. As an incorporated entity under German civil law, we are subject to the provisions of the [EU General Data Protection Regulation \(GDPR\)](#), the [Federal Data Protection Act \(BDSG\)](#), the [Telemedia Act \(TMG\)](#) and the [Telecommunication Telemedia Privacy Protection Act \(TTDSG\)](#). We have taken technical and organisational measures to ensure our compliance and the compliance of external service providers with the data protection regulation.

This website uses SSL – that is, TLS encryption – in order to protect the transfer of personal data and other confidential information (for example, orders or enquiries sent to the controller). A connection is encrypted if you see the character sequence 'https://' and the padlock icon in your browser's address bar.

### 1. The EnMAP Services

The German Aerospace Center DLR offers services for searching, viewing, ordering, and downloading EnMAP observations and products held in the German Satellite Data Archive (Deutsches Satellitendatenarchiv). These services are hereafter referred to as "EnMAP Services"; the data will be referred to as "EnMAP observations and products".

Since EnMAP observations and products are subject to license terms and conditions and in order to manage different roles and access rights, a personal account is required containing personal data of the user.

In order to access EnMAP observations and products, a user needs to register an account at the EnMAP Instrument Planning Portal (EnMAP IPP) and accept the EnMAP Acceptable Use Policy and Conditions of Use ("AUP"). The AUP is a contract between the user and DLR defining the rules and obligations regarding system access to EnMAP-IPP and serves as legal basis for storing the personal data of the user.

Some EnMAP roles allow the user to access the EOWEB® GeoPortal (EGP) in order to search, view, order and download observations and products from EnMAP and other missions.

During the registration process, DLR will collect personal information as specified in this document. DLR requires this information for contractual purposes and for other legitimate interests which are detailed below. The information collected will be stored and processed on DLR IT infrastructure located in the Federal Republic of Germany.

The EnMAP Services are generally aimed at persons aged 16 years or older.

### 2. Name and address of the controller

**Controller within the meaning of the GDPR** is the

Deutsches Zentrum für Luft- und Raumfahrt e. V. (DLR)  
Linder Höhe  
51147 Köln  
E-Mail: [datenschutz@dlr.de](mailto:datenschutz@dlr.de)

### 3. Name and address of the data protection officer

Contact details of DLR's Data Protection Officer:

Deutsches Zentrum für Luft- und Raumfahrt e. V.  
Uwe Gorschütz  
Dept. IT-LTG  
Linder Höhe  
51147 Köln  
Phone: +49 2203 601 4015  
E-Mail: [datenschutz@dlr.de](mailto:datenschutz@dlr.de)

### 4. Joint Controllershship

The EnMAP Services are provided by DLR and the GFZ Potsdam (EnMAP Scientific Principal Investigator) as Joint Controllers according to Art. 26 GDPR (see <https://www.enmap.org/mission/organization/>).

The essence of the Joint Controllershship arrangement (Art. 26 para. 2 GDPR) between DLR and GFZ is as follows:

DLR and GFZ collaborate to ensure that you can exercise your rights (see section 12) according to Articles 13 to 21 GDPR.

DLR is responsible for fulfilling the information obligation of Art. 13 and Art. 14 GDPR.

DLR will provide the information regarding Art. 15 GDPR to you upon request; both DLR and GFZ will contribute the information of their area of responsibility.

Point of Contact for all data protection matters is [datenschutz@enmap.org](mailto:datenschutz@enmap.org) (Art. 26 para. 1 GDPR).

### 5. Definition of terms

Among others, we use the following terms in this Data Protection Consent, set out in the General Data Protection Regulation and the Federal Data Protection Act:

#### *1. Personal data*

Personal data refers to any information relating to an identified or identifiable natural person (hereinafter: 'data subject'). An identifiable natural person is one who can be identified – directly or indirectly – in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

#### *2. Data subject*

A data subject is any identified or identifiable natural person whose personal data is processed by the controller.

### *3. Processing*

Processing is any operation or set of operations performed on personal data or on sets of personal data – whether or not by automated means – such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, deletion or destruction.

### *4. Restriction of processing*

Restriction of processing means the marking of stored personal data with the aim of limiting its processing in the future.

### *5. Profiling*

Profiling means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

### *6. Pseudonymisation*

Pseudonymisation means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

### *7. Controller or data processing controller*

Controller or data processing controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

### *8. Processor*

Processor means a natural or legal person, public authority, agency or other body that processes personal data on behalf of the controller.

### *9. Recipient*

Recipient means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities that may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients.

### *10. Third party*

Third party means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

### *11. Consent*

Consent of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

## 6. General information on data processing

### *a) Description and scope of data processing*

For the purposes of the EnMAP License Agreement and to manage system access to the EnMAP Services we collect, store and process the following personal data from you:

Mandatory data for self-registered users:

- First name,
- Last name,
- Email address,
- User name (user-id),
- User password,
- User postal address,
- User phone number.

Optional data for self-registered users:

- Title,
- Name of organization,
- Department within the organization,
- User category,
- Field of activity,
- Billing information including person, postal address, email address and phone number,
- Delivery information including person, postal address, email address, network address (for online delivery) and phone number.

The billing and delivery information must be filled for technical reasons and are pre-filled with the mandatory address information upon self-registration. You are free to change the billing and delivery information at any time using the account self-management functionality.

Furthermore, the following administrative data is stored in the internal database for the corresponding user profiles. These cannot be changed by the user:

- Internal user ID,
- Access rights of the user (e.g. access to specific datasets, quota information),
- Time of user profile creation and last user profile update,
- Information regarding online data delivery,
- Time of last login,

- Information regarding password policy,
- Information regarding the user registration, authentication method, identity provider,
- Password procedure, password history, and date of last password change,
- Timestamps of successive authentication errors.

For accounting and quota management purposes, quota-specific sub-accounts are created and maintained in order to allow the user to operate on a selected quota, using the personal data described above.

### *b) Legal basis for data processing*

The legal basis for the processing of your mandatory personal data is Article 6 paragraph 1 lit. b GDPR and Article 89 GDPR in conjunction with § 27 BDSG.

The legal basis for the processing of the administrative data is Article 6 paragraph 1 lit. f GDPR and Article 89 GDPR in conjunction with § 27 BDSG.

### *c) Purpose of data processing and duration of storage*

The purpose of data processing in the context of the EnMAP Mission is the processing for scientific research and archiving purposes in the public interest in the area of Earth Observation (Art. 89 GDPR in conjunction with § 27 BDSG).

DLR needs the mandatory registration data for the administration of the system access contract (Acceptable Use Policy and Conditions of Use, AUP) and the license agreement concluded with you, for example in order to be able to legally sanction violations of contract, such as unauthorized disclosure to third parties, or to be able to manage possible terminations.

You may enter the optional data in order to provide a complete postal address, in case the need for postal (non-electronic) communication arises. You are free to enter or delete the optional data at any time.

Your above-mentioned personal data will be stored on DLR's servers from the date of your online registration as a user.

Your personal data will be deleted or blocked as soon as the purpose of the processing no longer applies. This is the case if you or DLR terminate the system access contract (AUP) or the license agreement. Storage may also take place if this has been provided for by the European or national legislator in EU ordinances, laws or other regulations to which the person responsible is subject.

In addition, the system automatically sends you a reminder e-mail once a year. These reminder e-mails ask you to check the data stored about you and to correct it if necessary. They ensure that your personal data is up to date and that the contractual relationship, rights and obligations arising from the system access contract and the license agreement are brought to mind.

DLR may also use your e-mail address to contact you in case of security or other important issues.

If you no longer need the system access or the license, such an e-mail can also be a reminder of the possibility of terminating the system access contract or the license agreement and thus limit the system to the necessary in the interest of all parties.

Please note that the purpose of storing your e-mail address is to be able to contact you by e-mail until termination of your account. Therefore, the use of one-time e-mail addresses is not allowed.

Please contact us in case of changes in your e-mail address.

The administrative data is required by DLR for IT technical reasons, that is to say for the steering of the workflows in the system and for purposes of IT security, e.g. enforcement of the password guideline in respect to the term for password renewal, in respect to control of usage of old passwords, blocking of the account in case of several false registration attempts, etc.

This is also the legitimate interest for DLR in the sense of Article 6 paragraph 1 lit. f GDPR for processing of administrative data. When the account is deleted the administrative data will be deleted as well.

If you violate the license contract or your obligations stated in this data protection consent, DLR reserves the right to disable or delete your account without prior notice. In such cases your personal data can be stored until all legal claims are settled (Article 17 paragraph 3 lit. e GDPR).

## 7. Collaboration between EnMAP users, disclosure of personal data

### *a) Description and scope of data processing*

To participate in the EnMAP mission the collaboration between EnMAP users is essential. Depending on the EnMAP roles you apply for and get assigned to or if you submit observation proposals subject to scientific review,

- selected account and personal data might be disclosed to other EnMAP users, or
- selected account and personal data of other users might be disclosed to you.

The selected account and personal data (so-called “personal contact information”) that might be disclosed to other EnMAP users or to you comprises:

- Title
- First name, Last name
- Email address
- User name (user-id)
- Name of organization
- Department within the organization
- Country

Please note that *Title, Name of organization, Department within the organization* are optional attributes of your EnMAP user profile. You might leave these attributes empty if you do not wish to disclose this information.

The following table (also Table 3 in the EnMAP Collaboration Contract) summarizes the role-based disclosure of personal contact information between EnMAP users. The table can be read in two ways:

- The disclosure of your personal contact information to other users depending on your role is shown in rows: select your role in the left column (EnMAP user "A") and the respective rows shows to whom your personal contact information might be disclosed.
- The personal contact information of other EnMAP users that might be disclosed to you depending on your role is shown in columns: select your role in the first row ("EnMAP user "B") and the respective columns show whose personal contact information might be disclosed to you.

Role of EnMAP user A	Role of EnMAP user B								
	(none)	Cat-1		PI-AO		Reviewer			Internal
		Own AO <sup>1</sup>	Other AO	Own AO	Other AO	Own AO		Other AO	
						Assigned <sup>2</sup>	Not assigned		
(none)	no	no	no	no	no	no	no	no	no
Cat-1	no	Yes if agreed No otherwise	Yes if agreed No otherwise	Yes	Yes if agreed No otherwise	Yes	Yes	Yes if agreed No otherwise	no
PI-AO	no	yes	yes	(n/a)	yes	yes		yes	no
Reviewer	no	no	no	yes	yes	yes		yes	no
Internal	no	no	no	no	no	no		no	yes

Table 1: Role-based disclosure of personal contact information to other EnMAP users

<sup>1</sup> As the „own role“ is assigned on a per-AO basis, there is a difference between other users also related to that AO (“own AO”) and users that are not related to the AO the user has the role “Cat-1” for.

<sup>2</sup> Among those users with the role “Reviewer” for the same AO the user has the role “Cat-1” for, the respective user B is assigned as Reviewer to a proposal of Cat-1 user A”.



Please note that disclosure depends also on:

- If users are related to the same AO or not, and
- If a [Cat-1](#) user has decided to publish the personal contact information along with an individual proposal or not, and
- If a reviewer for an AO a user has submitted a proposal to is assigned to that proposal for review or not.

The only unique attribute of the personal contact information is the user name (user-id), as it is possible to register more than one EnMAP IPP account and apply for EnMAP roles on a per-account basis. Therefore, it is necessary to disclose the user name in order to unambiguously identify an user account.

The description and scope of the role-based disclosure of selected account and personal data is described in the EnMAP Collaboration Contract concluded with every EnMAP user.

The subset of disclosed personal contact information is limited to the extent required to achieve the purposes. Guided by the principle of data minimisation (Article 5 paragraph 1 lit. c GDPR) and based on the operational experiences made during the routine operations phase, the disclosure of personal contact information might be further limited if it turns out that the purposes can be achieved also on a reduced subset.

**DLR reserves the right to change the disclosure of reviewer contact information**, including the option of limiting the disclosure to own AOs or blind reviews.

#### *b) Legal basis for data processing*

The legal basis for the selective disclosure of your personal contact information to other EnMAP users in specific situations (as described in section 7.a) is the EnMAP collaboration contract concluded with you and is therefore Art. 6 para. 1 lit. b GDPR and Article 89 in conjunction with § 27 BDSG.

Other EnMAP users that process your personal contact information are acting under the authority of DLR (Art. 29 GDPR) and are legally bound to comply with the requirements of the applicable data protection regulations with regard to the confidentiality and integrity of personal data as stated in the EnMAP Collaboration Contract.

Access to your personal contact information is limited to the secure online EnMAP Portals which DLR provides as part of the technical and organizational measures taken to ensure an appropriate level of data protection.

The legal basis to make your personal contact information available to a receiving EnMAP user by DLR in order to achieve the desired EnMAP task is the Collaboration Contract concluded with the receiving EnMAP user in your interest in the sense of Art. 49 para. 1 lit. c GDPR.

The legal basis for the selective disclosure of personal contact information of other EnMAP users to you in specific situations (as described in section 7.a) is the EnMAP collaboration contract concluded with you and the the EnMAP user whose personal contact information is disclosed to you, and is therefore Art. 6 para. 1 lit. b GDPR and Article 89 in conjunction with § 27 BDSG.

### *c) Purpose of data processing*

The purpose of disclosing selected contact information is to allow the collaboration tasks between EnMAP users, to support the scientific exchange and to enable participation in EnMAP activities.

The purpose of the role-based disclosure of selected account and personal data is described in the EnMAP collaboration contract concluded with every EnMAP user.

### *d) Duration of storage*

As no additional personal data is stored for the role-based disclosure of selected account and personal data, duration of storage is not applicable.

## 8. Provision of the website and generation of log files

### *a) Description and scope of data processing*

Every time you visit the websites of the EnMAP Services, our system automatically collects data and information from the computer system of the calling computer.

The following data is collected:

- information about the browser type and version used
- the computer's operating system
- the IP address of the computer
- date and time of access

The data is also stored in the log files of our system. This data is not stored together with other personal data of the user.

### *b) Legal basis for data processing*

The legal basis for the temporary storage of data and log files is Art. 6 para. 1 lit. f GDPR.

### *c) Purpose of data processing*

The temporary storage of the IP address by the system is necessary to enable the website to be delivered to the user's computer. For this the IP address of the user must remain stored for the duration of the session.

The data is stored in log files to ensure the functionality of the website. In addition, the data serves to optimize the website and to ensure the security of our information technology systems. An evaluation of the data for marketing purposes does not take place in this context.

The pages providing the EnMAP Services collect a series of general data and information each time a person or an automated system accesses the Internet pages. This general data and information is stored in the log files of the servers. We may record (1) the browser types and versions used, (2) the operating system used by

the accessing system, (3) the website from which an accessing system accesses our website (so-called referrer), (4) the sub-websites which are accessed via an accessing system on our website, (5) the date and time of access to the website, (6) an Internet protocol address (IP address), and (7) other similar data and information which serve to avert danger in the event of attacks on our information technology systems.

When using this general data and information, DLR does not draw any conclusions about the person concerned. Rather, this information is required to (1) correctly deliver the contents of our website, (2) ensure the integrity of the contents of our website, (3) ensure the long-term functionality of our information technology systems and the technology of our website, and (4) provide law enforcement authorities with the information necessary for criminal prosecution in the event of a cyberattack. These anonymously collected data and information are therefore evaluated by DLR both statistically and with the aim of increasing data protection and data security in our research center in order ultimately to ensure an optimum level of protection for the personal data processed by us. The anonymous data of the server log files are stored separately from all personal data provided by a person concerned.

Our legitimate interest in data processing according to Art. 6 para. 1 lit. f GDPR also lies in these purposes.

#### *d) Duration of storage*

The data will be deleted as soon as they are no longer necessary to achieve the purpose for which they were collected. In the case of the collection of data for the provision of the website, this is the case when the respective session has ended.

If the data is stored in log files, this is the case after fourteen days at the latest. Further storage is possible. In this case, the IP addresses of the users are deleted or garbled, so that an assignment of the calling client is no longer possible.

#### *e) Possibility of objection and elimination*

The collection of data for the provision of the website and the storage of data in log files is absolutely necessary for the operation of the website. Consequently, there is no possibility of objection on the part of the user.

## 9. Registration form

### *a) Description and scope of data processing*

During the user account self-registration process the personal information described in section "Personal data to be provided during user registration" above is collected in an account registration web form.

The data is also stored in the log files of our system. This data is not stored together with other personal data of the user.

### *b) Legal basis for data processing*

The legal basis for the temporary storage of the registration data is Art. 6 para. 1 lit. b GDPR.

*c) Purpose of data processing*

The temporary storage of the registration data by the system is necessary to create the user account. We can use this data for helpdesk purposes, e.g. in case of user requests due to self-registration problems.

*d) Duration of storage*

All statements of the section "Provision of the website and creation of log files" above apply. Data stored in log files are deleted after fourteen days at the latest.

## 10. Use of cookies, web storage and similar technologies

*a) Description and scope of data processing*

Our website uses technically necessary temporary cookies.

Cookies, web storage and similar technologies provide websites with methods for storing client-side data. Cookies are text files which are stored on a computer system via an Internet browser. Web storage is a more modern and standardized way of storing information on the client side (in the Internet browser).

Many websites and servers use cookies, web storage and similar technologies. The information that is stored on the client side often contain an unique identifier (ID), in the case of cookies a so-called cookie ID. This enables the visited Internet pages and servers to distinguish the individual browser of the person concerned from other Internet browsers that contain other IDs. A particular Internet browser can be recognized and identified by its unique ID.

So-called session cookies (or session web storage) are used for registration and login and further access to the personalized area of the site. The use of session cookies is required for the secure transmission of user input from the web form to the DLR server. The session cookies become invalid max. 10 hours after the last user input or after the active logout of the user. The technically necessary session cookies are only used for the above-mentioned purpose and not, for example, to analyze user behavior (user tracking).

*b) Legal basis for data processing*

The legal basis for the processing of personal data using technically necessary cookies is Art. 6 para. 1 lit. f GDPR.

*c) Purpose of data processing*

The purpose of using technically necessary cookies, web storage or similar technologies is to ensure the secure transfer of user permissions from the web forms to DLR servers and databases. The user data collected by technically necessary cookies are not used to create user profiles.

### *e) Duration of storage, possibility of objection and elimination*

The person concerned can prevent the setting of cookies or the use of web storage by our website at any time by means of an appropriate setting of the Internet browser used and thus permanently object to the setting of cookies or the use of web storage. Furthermore, client-side data that has already been stored can be deleted at any time via an Internet browser or other software programs. This is possible in all common internet browsers.

If the person concerned deactivates the setting of cookies or web storage in the Internet browser used, not all functions of our Internet site are fully usable.

## 11. Access to the data by third parties

To create and manage the necessary IT systems and the servers, DLR contracts with external IT service providers, who are granted access to the users' personal data stored in the system as part of their work for DLR, in particular as part of system administration.

The IT service providers are the following:

- Computacenter AG & Co. oHG  
Europaring 34-40  
50170 Kerpen
- Werum Software & Systems AG  
Wulf-Werum-Straße 3  
21337 Lüneburg
- Navum GmbH  
Am Anger 3  
82237 Wörthsee

DLR has concluded contract data processing agreements with these companies, which oblige these companies to comply with the requirements of data protection law and ensure DLR's right to monitor compliance with these requirements. Your personal data will neither be transmitted to other third parties nor to third countries.

## 12. Rights of the data subject

If your personal data are processed, you are a data subject within the meaning of the GDPR and you have the following rights against the controller in accordance with the following provisions:

(1) Pursuant to Art. 15 GDPR, you may request **information** about the personal data we process. In particular, you may request information about the purposes of processing, the category of personal data, the categories of recipients to whom your personal data have been or will be disclosed, the planned storage period and the existence of the rights explained in this section.

(2) Pursuant to Art. 16 of the GDPR, you may request the **rectification** of inaccurate or incomplete personal data held by us without undue delay.

(3) Pursuant to Art. 17 of the GDPR, you may request the **erasure** of your personal data stored by us, unless the processing is necessary for reasons specified by law, in particular to exercise the right to freedom of expression and information, to comply with a legal obligation, for reasons of public interest or to assert, exercise or even potentially defend legal claims.

(4) Pursuant to Art. 18 GDPR, you may request the **restriction of the processing** of your personal data insofar as their accuracy is disputed by you, the processing is unlawful, but you object to their erasure and we no longer require the personal data, but you need them for the assertion, exercise or defence of legal claims or you have objected to the processing pursuant to Art. 21 GDPR.

(5) Pursuant to Art. 20 GDPR, you may receive the personal data you have provided to us in a structured, commonly used and machine-readable format or request that it be **transferred** to another controller.

(6) Pursuant to Art. 7 (3) GDPR, you may **revoke** a consent granted under data protection law at any time vis-à-vis us. This has the consequence that we may no longer continue the data processing based on this consent in the future.

#### **(7) Right of objection pursuant to Art. 21 GDPR**

**If personal data is processed on the basis of legitimate interests pursuant to Art. 6(1) lit. (f) of the GDPR, you have the right to object to the processing of your personal data pursuant to Art. 21 of the GDPR, provided that there are grounds for doing so which arise from your particular situation or the objection is directed against direct marketing. In the latter case, you have a general right to object, which is implemented by us without specifying a particular situation, unless the processing is necessary for the performance of a task carried out in the public interest, Art. 21 (6) of the GDPR.**

For the purpose of exercising these rights, please contact the office indicated in section 4 above.

(8) Pursuant to Art. 77 of the GDPR, you may lodge a complaint with a supervisory authority. As a rule, the supervisory authority of your usual place of residence or workplace or the registered office of the controller is available for this purpose.