

RECORD OF PROCESSING OPERATION¹ ON

EEA SDI: The EEA catalogue of geospatial datasets

Nr.	Item	Description
1.1	Reference number	DP.IT.20.2_SDI Catalogue
1.2	Name and contact details of controller	The SDI Data Controller is the Head of Group of DIS2 - Data Management group within the DIS programme (Data and Information Services). The SDI mail box is the following: sd@eea.europa.eu
1.3	Name and contact details of joint controller(s) (where applicable)	N/A
1.4	Name and contact details of the processor (where applicable)	The SDI external contractor (Specific Contract 3325-B2020-EEA-58005 implementing Framework Service Contract EEA/DIS/19/002/LOT 2, coordinated by KU Leuven, contact point DannyVandenbroucke danny.vandenbroucke@kuleuven.be), which may have access to and eventually process information stored at the SDI on behalf of the EEA.
1.5	Name and contact details of the DPO	DPO@eea.europa.eu
1.6	Purpose of the processing	<p>The EEA SDI¹ is a public information system based on a metadata catalogue service that facilitates the discovery of the geospatial datasets produced and/or published by the EEA. Through the metadata, users can access information on the content and quality of the datasets, and ultimately download the datasets and supporting documents (quality reports, methodologies) if available. While public datasets and related public documents can be downloaded by any user, restricted or internal datasets can only be accessed by EEA staff and their partners under authentication. In the SDI there are currently two catalogue instances available: the “EEA public catalogue²”, which is the reference catalogue with the metadata information on the geospatial datasets and a “metadata editor³” that allows users to create their own metadata following the EEA guidelines.</p> <p>Metadata are created, provided and stored following the EEA metadata profile⁴, which is fully compliant with ISO 19115:2003 and ISO/TS 19139:2007 standards and INSPIRE Directive and Implementing Rules.</p> <p>For authenticated users, the SDI also provides access to internal data sets described by the metadata files mentioned above (with the exception of restricted datasets with limited use licenses) and associated documents.</p>

¹ Record of EEA activities processing personal data, based on Article 31 of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC.

1.7	Description of categories of persons whose data the EEA processes and list of data categories	<p>For the purposes detailed above, it is required that some basic information about the organisations and individuals acting as a contact point, owning, maintaining, processing or publishing the geospatial dataset, or creating the metadata, is included in the metadata (name, phone, email address), as contact details for the users of the dataset. The minimum information requested to be compliant with the abovementioned standards are organisational name and contact email, but data providers may opt to provide more information such as individual name, phone number or address.</p> <p>Personal data such as names, e-mail addresses and affiliation may be included in supporting (public) documents made available on certain cases together with the dataset (typically quality reports or documents about methodological processes). This personal data normally corresponds to the name of author, co-author or reviewers of the report. The decision of the publication of reports through the EEA SDI falls only under the responsibility of the EEA staff in charge of the related dataset and/or the related report.</p> <p>EEA staff, ETCs or contractors working on behalf of the EEA need to use their EIONET account to access the metadata editor or to download internal datasets through the SDI. The personal data requested for creating an Eionet account is listed in the “Eionet Privacy Statement”: What personal information we collect and for what purpose.</p> <p>Once authorised, users can create metadata using the metadata editor, or download any internal datasets from the SDI, both of which may include some personal data as indicated above.</p> <p>The personal data collected and processed as part of the actual metadata may refer to any person which is a point of contact for the dataset the metadata describes and/or is involved in the creation, publication or processing of that specific dataset or the corresponding metadata. In the case of supporting documents provided with the datasets through the SDI, the personal data included refers typically to those involved in the creation or review of the document itself. Typically, these documents are for public use, unless it is stated otherwise (in which case it can only be accessed under authentication).</p> <p>Finally, “transactional data” of any visitor of the SDI web page is also processed; this data refer to IP address, browser version and device information that is part of the various internet communication protocols and is necessary to securely deliver web pages to the internet client.</p>
1.8	Time limit for keeping the data	<p>The personal data provided for creating the Eionet account are kept as long as the subject does not ask for the account to be deleted, as explained in the Eionet Privacy Statement: “How long do we store your personal data”.</p> <p>The personal data provided as part of the metadata, or included in supporting documents, are kept until the end of the lifecycle of the SDI system or as long as the contact point for the metadata or the dataset decides to cease the right of making them available through the SDI.</p>

		<p>Transactional data (security logs) is stored for a maximum of 1 year for security audit purposes unless there is an individual reason to keep information for a longer period of time (e.g. when individual IP addresses are blocked if part of a DoS-attack).</p>
1.9	Recipients of the data	<p>For the purposes detailed above, and as a public information system, personal data (e.g. contact details) eventually included in the metadata files can be accessed by anyone consulting the catalogue.</p> <p>The catalogue interface is publicly available and the full content of their metadata can be harvested by other catalogues sharing the same standard interface. Currently, the SDI is harvested regularly by the catalogue of GEOSS (https://www.geoportal.org/) and the Copernicus Portfolio portal (https://services-portfolios.copernicus.eu/) so any change in the SDI reverts into these catalogues.</p> <p>As previously stated, personal data included in internal datasets or documents available through the SDI can only be made accessible to EEA staff and non-EEA staff (ETCs or EEA contractors acting on behalf of EEA) having an EIONET account and who have been granted access on demand.</p> <p>Transactional data mentioned above are also processed by personnel at EEA and at CERT-EU⁵, which provides security services for EEA. These transactional data are also available to our Internet Service Provider (tdc.dk) and our cloud provider Amazon in EU, therefore for them, their privacy policies apply.</p> <p>Other documents and material produced in relation to the SDI may also be disclosed to the public subject to the provisions contained in Regulation (EC) No 1049/2001 of the European Parliament and of the Council of 30 May 2001 regarding public access to documents.</p> <p>The SDI also uses the external service openstreetmap.org for background maps and other services. Therefore, transactional personal information such as IP-address, browser version, operating system, referring web page, data and time of page visits and the pages accessed are also made accessible to the data controller behind openstreetmap.org services. The data policy behind the use of Openstreetmap services is described here: https://wiki.osmfoundation.org/wiki/Privacy_Policy</p> <p>#Data_we_receive_automatically.</p> <p>No personal data is shared with third parties for direct marketing purposes.</p>
1.10	Are there any transfers of personal data to third countries or international organisations? If so, to which ones and with which safeguards?	No

1.11	General description of security measures (where possible)	<p>Access to personal data is subject to strict security controls like encryption and access control.</p> <p>As indicated above, full access to <u>internal datasets</u> and related documents as well as to the metadata editor requires authentication. Access is only granted to EEA staff (by default) and, additionally, to non-EEA staff (ETCs or EEA contractors acting on behalf of EEA) with an EIONET account (the latter only on demand as they need to become members of the Eionet SDI Group (eionet-group-sdi)).</p> <p>The functioning of the servers and databases containing the personal data is compliant with the EEA's Information Security Policy and the provisions established by the EEA's Information Security Officer.</p>
1.12	Measures for providing additional information, including how data subjects may exercise their rights of access, rectification, data portability (where applicable), etc.	<p>Authorised users of the EEA catalogue and/or the metadata editor have the right to get the EIONET account deleted from the dedicated Directory by sending an email to <i>Eionet</i> Helpdesk: helpdesk@eionet.europa.eu.</p> <p>Anyone acting as a contact point, owner, publisher, processor, etc., for a specific dataset and which personal data is made available in the metadata can ask to be deleted by contacting the SDI Team via email: sdi@eea.europa.eu. This email is available in all metadata files. The request will be handled within maximum 15 calendar days. The SDI Team will contact the catalogues harvesting the SDI catalogue to request a new harvesting of the metadata without the personal data asked to be deleted.</p> <p>SDI specific Privacy statement is available under "Privacy Policy" on the SDI web page https://sdi.eea.europa.eu/</p>