Privacy statement for DLR

About the privacy statement

This privacy statement describes how the data controller processes your personal data in the service. The purpose of this privacy statement is to inform you about what personal data we process, how it is processed, who is responsible for the processing, what your rights are and who you can contact.

What are personal data?

Personal data are all forms of data, information and assessments that can be linked to you as a person, cf. the GDPR Article 4 (1). The decisive factor as to whether data constitutes personal data is whether it can be linked to a specific person. Data that, on its own, cannot be linked to an individual person may constitute personal data in cases where the data are found together with other data.

The service in brief

DLR is a service for the storage, retrieval, publication and sharing of digital learning resources and will normally interact with the data controller's other services for registering, publishing and presenting the resources, e.g. digital learning platforms, and storage and streaming services.

The service registers metadata about the resources and defines access rights at the institution, group and user levels. The resource content may be stored in external storage services, such as file systems or online and be referred to by a URL. The data controller defines the users and access rights for maintenance and management of the resources. The service can include external storage services if defined in the service agreement.

The service comprises a web client for the presentation/consumption of resources, and the management of registered resources and configuration of the service. The web client for presentation of the resources can be integrated with the learning platform via LTI web links or third party integrations.

The service does not allow processing of sensitive personal data.

The purpose of personal data processing in the service

The service registers different types of persons and pertaining data for the following purposes:

Types	**Description**	**Purpose of processing**

System administrator	The system administrator holds all rights to the service and defines users with top-level administrator access for the data controller.	The data processor's administration of services.
Administrator	The administrator is the data controller's top-level administrator and defines new users with rights and roles for the administration and use of the service.	The data controller's administration of services.
Technical personnel	Support users and technical users defined by the data controller.	For assistance with and monitoring of the service.
Resource managers	Curator (subject responsibility), editor (legal responsibility), resource owner (person who has registered a resource). The publisher is also registered for the resource, but this is typically the data controller's organisation and not a person.	For administration and maintenance of the resources.
Authenticated users	Employed at the institution or an invited person. Has restricted rights but can add new resources and access resources that are shared with the user.	Registration of resources and consumption of open resources or resources shared with the user.
Non-registrated users	Persons who use the service without logging in. IP addresses will be registered in the log.	Consumption of open resources.
Metadata – persons related to registered resources.	Metadata about the resource, such as the author.	Cataloguing, crediting and accountability of the persons behind the publication
Bibliographic data – persons referred to in the content	Personal data referred to in the content, such as in biographical material. Indirectly processed in the service and directly if the storage service is set up as part of the service.	To provide content to the public.

Registered personal data, legal grounds and storage time

Personal data related to user accounts in the service requires consent as legal grounds, cf. the Personal Data Act, and the GDPR Article 6(1)(a).

Registered personal data about authors, contact persons and non-registrated user are covered by the Personal Data Act, and the GDPR Article 6(1)(f) – to perform a task on grounds of legitimate interests.

The service does not allow processing of sensitive personal data. In the cases where the users themselves can write information in the comments field and similar, the user is obliged to meet the requirements and guidelines for the service. Users are not permitted to register sensitive personal data about themselves or others or to use the service for defamatory conduct.

The data controller is entitled to store information for statistical purposes, if this is in the interests of society at large, cf. the Personal Data Act Section 8 and the GDPR Article 6(1)(e).

The following personal data are processed in the service.

User data

Type of data	**Description**	**Source**
Basic user data	Full name	Feide
Contact information	Email address assigned by the organisation.	Feide
Profile	User's preferences in use of the service. Language preferences	Settings in DLR

Technical user data

Type of data	**Description**	**Source**
System identities	Unique identity for users of the service and integrated system.	Feide or other authentication services
System roles and affiliation to the organisation	The user is assigned roles in the system in order to provide adapted functionality and access to the service.	Feide, DLR

Session information and cookies	Information related to the user's dialogue with the service. Necessary to adapt functionality in the service and to authenticate users. We use an external analysis service to further develop and administer the service. Information from the end user is anonymised before it is analysed.	DLR, Feide, Dataporten, Google Analytics
Log	Log of system use related to the logged-in user and/or their IP address. The purpose of logs is to ensure security and integrity in the system, provide user support and analyse use of the service. The data collected include time of use, information about browsers and hardware, session information and other information that browsers normally provide.	Set up in DLR

Other personal data

Type of data	**Description**	**Source**
Metadata about the publication	Full name and role of author, co-author, editor, supervisor.	Set up in DLR or harvested as a result of user preferences
Personal data in the publication itself	Persons identifies in the publication Content is quality assured by the person responsible for publication.	Storage service for referred resource.

Information about your activity is stored in order to provide user support and give an impression of general use of the service.

Personal data is stored until one of the following occurs:

- User consent is withdrawn
- The purpose of the personal data processing has been fulfilled
- The data controller decides to discontinue the service

Logs and backups of the system data are stored for up to one year.

Users who register resources are linked to the resources by name for the life span of the resources.

Automatic case processing

Personal data related to the system users will not be subject to automated case processing or profiling.

Open personal data related to the publications can be subject to profiling of services that harvest information from the service, but will not be profiled as part of the service.

Disclosure of your personal data to third parties

Disclosure or export of data is defined as all disclosure of data aside from to the service's own system/processing or to the data subjects themselves, or to someone who receives data on their behalf.

Personal data linked to users are transferred in the following cases to countries outside the EU/EEA:

- When using social media logins such as Twitter, Facebook or LinkedIn, user information is transferred between the service and social media login service. Twitter, Facebook and LinkedIn are companies registered in the USA.

The service is run on servers in the EU/EEA.

Your personal data will be disclosed to Unit, which is the service provider, and to its subcontractors.

Subcontractors	**Function**
Blue Safespring AB	Cloud management and backup for Unit's direct services
UNINETT AS	Delivers Dataporten, for authentication of users of the services

Subcontractors	**Function**	**Affiliation (Country)**	**Processing of personal information outside EU/EEA**

AWS	Cloud management and backup for Unit's direct services	American company, but are hosted in Irland	No
Blue Safespring AB	Cloud management and backup for Unit's direct services	Norway and Sweden	No
UNINETT AS	Delivers Dataporten, for authentication of users of the services	Norway	No

The subcontractors' staff who need the personal data to perform their work will have adapted access in order to provide on-site maintenance, user support and any rectification of errors in the service.

Open personal data linked to the publications are openly shared with external services.

See the following table for the service's integrations.

Integration	**Purpose**
Authentication services	DLR is integrated with Feide Dataporten, which is provided by Uninett AS, and supports authentication via Twitter, Facebook and LinkedIn (all of which are registered under Privacy Shield in the USA). When using a social media login, the user must have accepted the terms and conditions of the external service.
The data controller's learning platform	Presentation and consumption of digital learning resources adapted to the user. The learning platform exchanges user ID with the service to filter the resources.
Export of metadata from DLR to other services defined by the data controller.	Transfer of resources to the data controller's other services for presenting or cross-registering resources, e.g. to Oria to facilitate retrieval.
Import of metadata to DLR from services defined by the data controller.	Transfer of resources from the data controller's other services for registration in DLR.
Felles autoritetsregister (Joint authority register)	Harvesting of authors from Felles autoritetsregister (service provided by the data processor), and registration of new authors in this register.

DOI and DataCite	The registrar for resources in the service can request a Document Object Identifier (DOI) to be assigned. This means that selected metadata, including the author's connection to the title, are published in DataCite, which is a source that is regularly harvested by search engines.

Security in relation to your personal data

Personal data processed in the service are secured by several measures. All transfers to and from the service related to user accounts are encrypted. The data processor conducts regular risk and vulnerability analyses and tests the security of the service to ensure your personal data are safe.

The data controller is responsible for procedures that address data protection in connection with the publication of content.

Your rights

Right to information and access

You have a right to receive information about how your personal data are processed in the service. This privacy statement has been produced to provide the information you have a right to receive. You also have a right to see/access your personal data that are registered in the service, and other personal data that are collected after you have actively logged in. You also have the right to request to receive a copy of your personal data.

A self-service solution in the service where users can see their personal data after logging in allows users to exercise their right of access. If the service does not provide complete information via the self-service solution, users can send a written enquiry to the data controller's user support to acquire access to more detailed information.

Right to rectification

You have a right to have inaccurate personal data about you rectified. You also have a right to have incomplete personal data about you supplemented. If you feel that the service shows inaccurate or incomplete personal data, please contact the data controller, stating the reason why the personal data are inaccurate or incomplete.

Please note that there is a limited possibility of rectifying data that are distributed via open interfaces.

Right to restriction of processing

In certain cases, you may have a right to request restrictions on the processing of your personal data. Restricted processing means that the personal data will still be stored, but that other processing in the service is restricted. To request restricted processing of personal data, the conditions in the Personal Data Act and the GDPR Article 18 must be met. You can request restricted processing

- Pending the data controller rectifying inaccurate or incomplete personal data
- If you have submitted an objection to the processing (see below for more details)
- If the personal data are necessary to establish or defend a legal claim

If restricted processing is granted, the data controller will notify you before the restriction is lifted.

Right to erasure

You have the right to demand that we erase personal data about you. If you would like your personal data to be erased, please contact the data controller. It is important that your request states why you want your personal data erased and, if possible, what personal data you wish to be erased.

Please note that legislation provides exemptions from the right to erasure in some cases. This could be cases where we process personal data to fulfil a statutory duty or to address important social interests, such as archiving, research and statistics.
Please note that there is a limited possibility of erasing personal data that are distributed via open interfaces.

Right to object

You have a right to object to processing of your personal data on certain conditions defined in the GDPR Article 21. This applies if:

- Legal grounds for the processing of personal data are based on legitimate interests, reasons of public interest or when exercising public authority
- Processing of personal data entails direct marketing or profiling
- Personal data are processed for scientific or historical research purposes or statistical purposes

The service does not generally satisfy these conditions, with the exception of the processing of author information and in cases where personal data are used for statistical purposes. When personal data are used for statistical purposes, the data are anonymised.

However, please note the following:

- If there is a special need to stop the processing, for example if you have a need of protection, or a confidential address or similar, please contact the data controller.
- When you have consented to the processing of personal data, you have a right to withdraw your consent.

Right to complain about the processing

If you feel that we have not processed personal data in a correct or lawful manner, or if you feel that you have been unable to exercise your rights with us, you have a right to complain about the processing. See our contact details below.

If we do not uphold your complaint, you have the possibility of filing a complaint with the Norwegian Data Protection Authority. The Data Protection Authority is responsible for ensuring that Norwegian enterprises comply with the provisions of the Personal Data Act and the GDPR in their processing of personal data.

Contact

The data controller
The institution is the data controller for personal data in the service and is the primary contact for end users.

The data processor
Unit develops and manages the service on behalf of the data controller and has the role of data processor.

Unit user support's contact details
Email: kontakt@unit.no