



DuraSpace FAIRness and GDPR

Tim Donohue, Michele Mennielli, David Wilcox



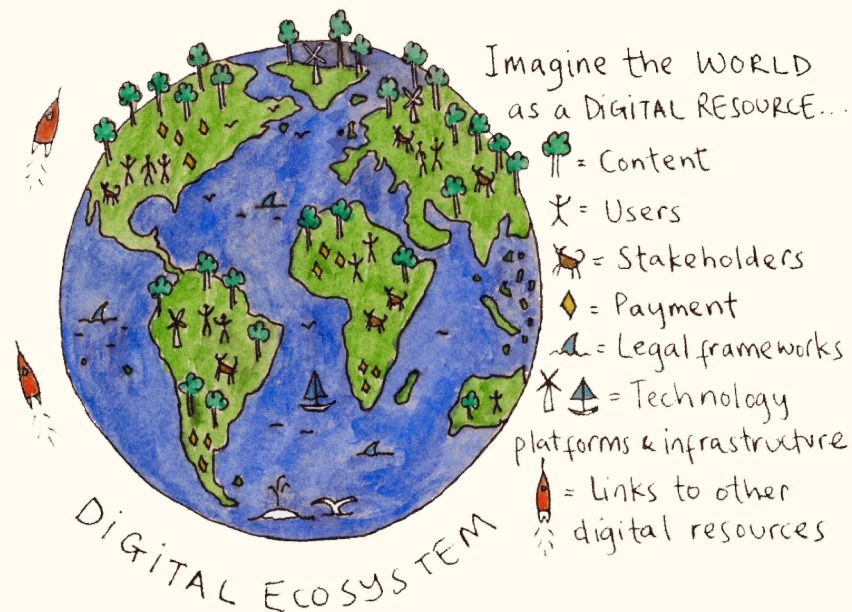
This work is licensed under a [Creative Commons Attribution 2.0 Generic License](https://creativecommons.org/licenses/by/2.0/).

About DuraSpace

DuraSpace is not for profit organization that provides leadership and innovation for **open technologies**

We work to ensure that **current and future generations** have **durable and persistent access** to our **collective digital heritage**

Our **community** is part of an **interconnected, worldwide, scholarly ecosystem**

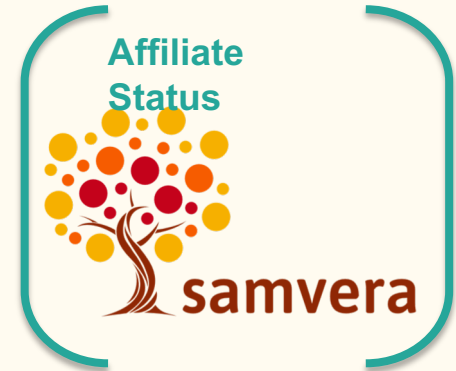


...its open source projects

DuraSpace open source projects are
part of the scholarly ecosystem



Fedora™



...its service providers



DURASPACE[™]

CRIS2018 | Umeå, June 2018

...its services

DuraSpace services are
part of the **scholarly ecosystem**

D SPACE DIRECT


DURACLOUD™

@archivesDIRECT

DURASPACE™

CRIS2018 | Umeå, June 2018

...its partners



CHRONOPOLIS



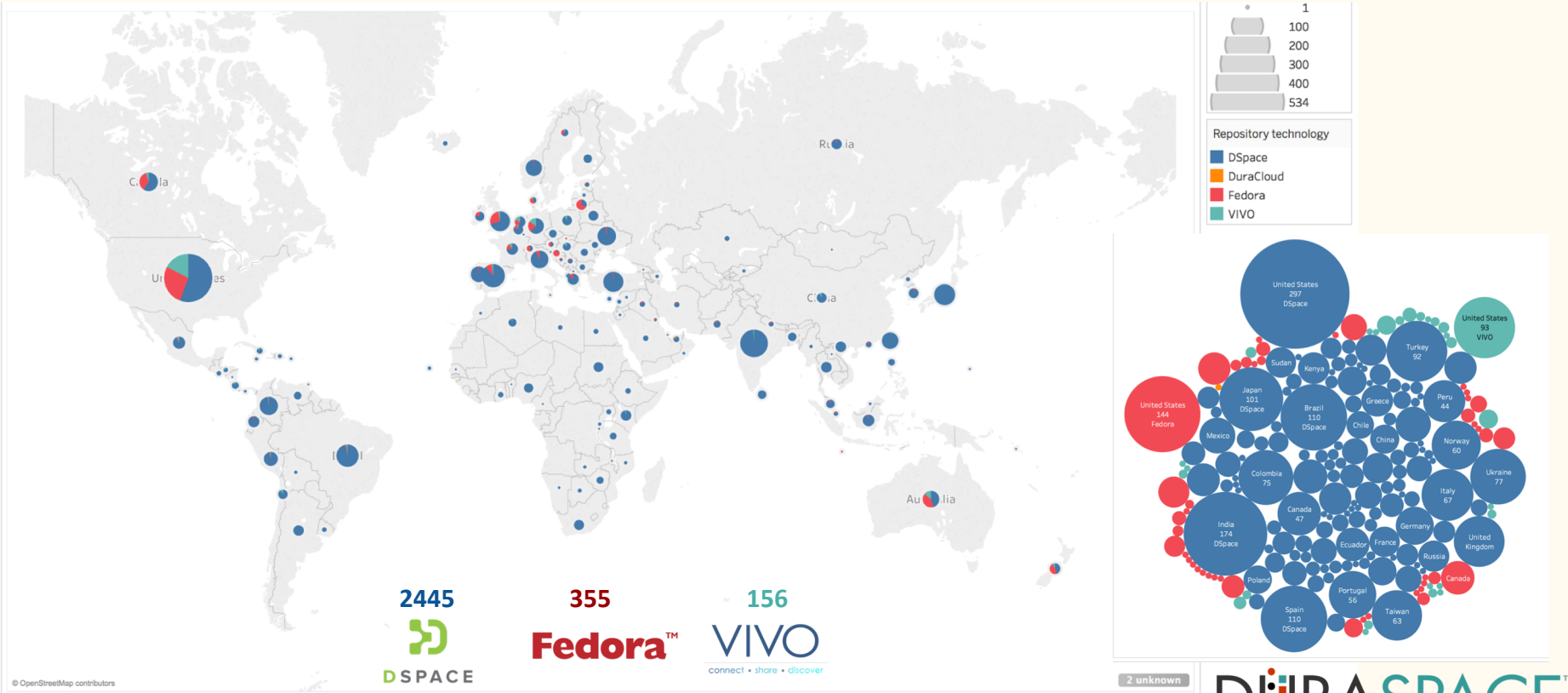
...its members



DURASPACE™

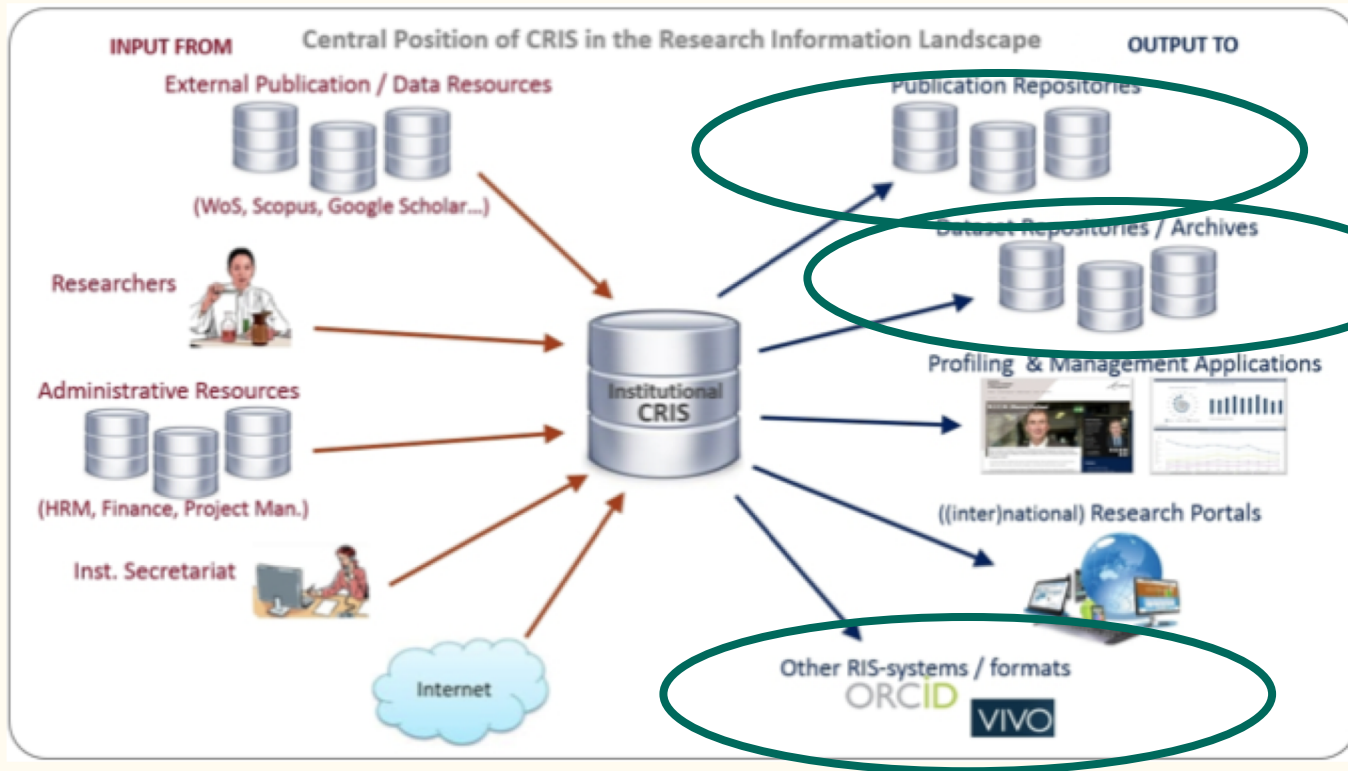
CRIS2018 | Umeå, June 2018

...and most importantly, its community!



*Based on the DuraSpace Registry

DuraSpace and the Research Information Ecosystem



What about FAIR data?

Findable

F1. (meta)data are assigned a globally unique and eternally persistent identifier.

F2. data are described with rich metadata.

F3. (meta)data are registered or indexed in a searchable resource.

F4. metadata specify the data identifier.

Features

DSpace

- / HTTP URIs
- / Store Handles and/or DOIs (external ids)
- / Extendable metadata schemas (QDC-based)
- / Findable via a built-in Solr search & search engine optimized (Google and Google Scholar)

Relevant

Fedora

- / HTTP URIs
- / PIDs as RDF properties
- / Support for any metadata
- / External indexing: Solr, Fuseki, etc.

Accessible

A1. (meta)data are retrievable by their identifier using a standardized communications protocol.

A1.1. the protocol is open, free, and universally implementable.

A1.2. the protocol allows for an authentication and authorization procedure, where necessary.

A2. metadata are accessible, even when the data are no longer available.

Features

DSpace

- / HTTP REST-API (major enhancements in v7)
- / Fine-grained, object-level Access Controls
- / Item landing page with metadata (and optionally binaries)

Relevant

Fedora

- / HTTP REST-API
- / Support auth via W3C Web Access Control
- / Containers and binaries

Interoperability

11. (meta)data use a formal, accessible, shared, and broadly applicable language for knowledge representation.

12. (meta)data use vocabularies that follow FAIR principles.

13. (meta)data include qualified references to other (meta)data.

Features

DSpace

- / Multi-lingual support
- / Controlled vocabulary / Authority control support
- / References in metadata via URIs, identifiers

Relevant

Fedora

- / Multi-lingual support
- / Ontology and vocabulary support
- / RDF links

Reusable

R1. meta(data) have a plurality of accurate and relevant attributes.

R1.1. (meta)data are released with a clear and accessible data usage license.

R1.2. (meta)data are associated with their provenance.

R1.3. (meta)data meet domain-relevant community standards.

Features

DSpace

- / Extendable metadata schemas (QDC-based)
- / Required deposit license (CC optional)
- / Provenance in metadata
- / Metadata input / validation is customizable

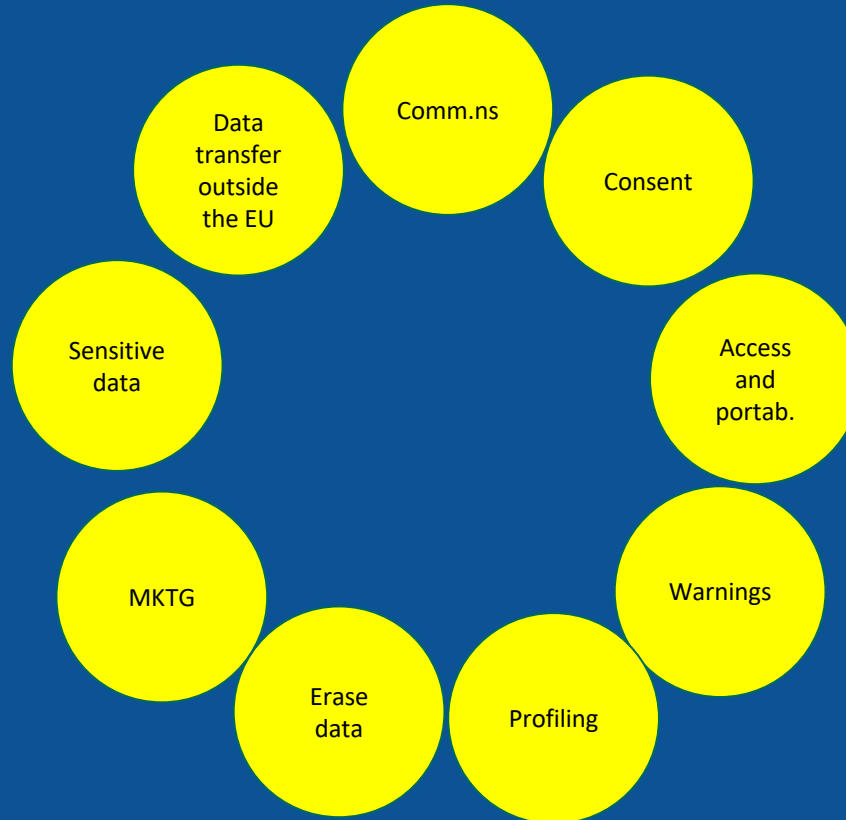
Relevant

Fedora

- / Rich metadata support
- / RDF links to licenses
- / Audit service
- / Metadata validation as a service

What about General Data Protection Regulation?

GDPR - protects the rights of people giving you their data



GDPR - Impact on the Repository

Comm.ns

Consent

Access
and
portab.

warnings

profiling

Erase
data

Must clarify
who's using the
data, why and
how

In case of
analysis and BI
activities?

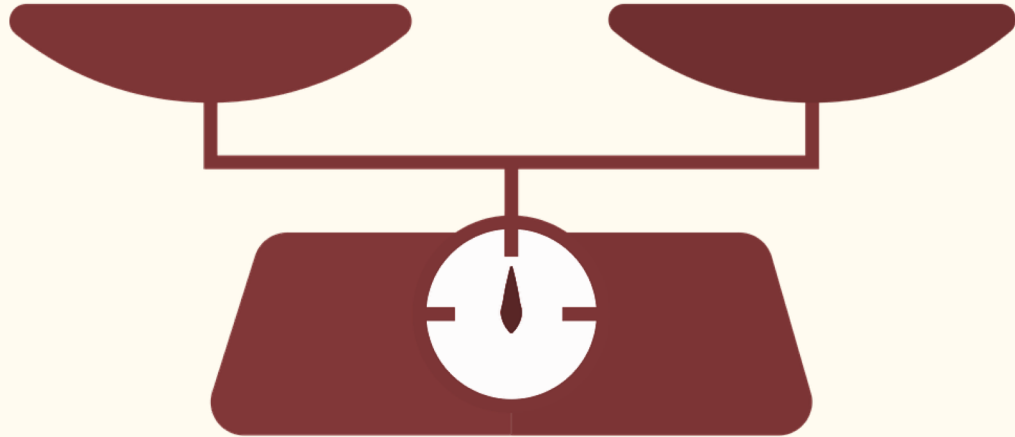
Interoperability
and standards?

Data breaches
to the users?

In the case of
analysis?

Public domain?

GDPR - Technology Vs Administration



GDPR

DSpace is drafting a guide/notes on "Data Protection & Privacy" on the Wiki at:

<https://wiki.duraspace.org/display/DSPACE/Data+Protection+and+Privacy>

Data Protection and Privacy

 Created by [Claudia Jürgen](#), last modified by Bram Luyten (Atmire) on May 07, 2018

Note: This article touches legal topics and no warranty is made about the accuracy. Please consult your data protection officer or law department to get advice.

A couple of issues have arisen with regards to data protection and especially with the new EU General Data Protection Regulation see [DS-3653](#). As DSpace is used all over the world the law and other requirements e.g. for certification vary from place to place. This page is intended to document how we use/store what kind of data and then help us identify issues and make things configurable, so that people can meet their obligations. Maybe it can help establish a data privacy policy for DSpace in general.

- [Actual State Analysis - What do we store and how do we process it.](#)
- [Proposals of Change and Future Default Behaviour](#)
- [Requirements of different regions/countries/organizations](#)
 - [Legal Requirements](#)
 - [Europe - General Data Protection Regulation](#)
 - [Email Template: Informing Registered DSpace Users](#)
 - [Other Requirements](#)
 - [German Initiative for Network Information - Repository Certification](#)
- [Tickets](#)



Thanks!
Questions?

Tim Donohue, Michele Mennielli, David Wilcox



This work is licensed under a [Creative Commons Attribution 2.0 Generic License](https://creativecommons.org/licenses/by/2.0/).