San Raffaele Open Research Data Repository (ORDR) is an institutional platform which allows to store, preserve and share research data. ORDR is powered by the Digital Commons Data repository platform.

Why use Digital Commons Data?

Open or restricted access to contents, with persistent unique identifiers to enable referencing and citation:
- When datasets are uploaded on Digital Commons Data, a DataCite DOI is reserved, which will become active upon publication of the dataset to enable citation.
- Datasets can be licenced under a range of open licenses.
- When data cannot be fully made open for legitimate reasons, it may be published
  - as a Restricted-Access dataset, where the files must be requested by the researcher, and the author can decide whether to act on the request, or
  - as a Metadata-Only dataset, where the files will not be deposited, in case they are too sensitive, or too large to be held on a repository.

Metadata to enable discovery and reuse:
- Every dataset can be annotated with a comprehensive set of metadata fields, including title, general description, description of each file, steps to reproduce the analyses, license, and administrative metadata such as institution and category.
- Institutions may provide additional custom metadata fields to be completed by their researchers.
- Links can be created to further associated research outputs, such as datasets, software or articles.
- To facilitate discovery and reuse of data, dataset metadata is available in the Dublin Core format and Schema.org format, conforming to the Google Dataset standard.
- Dataset metadata is also made available for harvesting via OAI-PMH endpoints.

Safeguarding integrity and authenticity of deposited data:
- Files deposited to Digital Commons Data are stored with Amazon S3, part of Amazon Web Services (AWS).
- Automated database backups happen every day whilst online, with a retention period currently set to 7 days. These backups are stored in the relevant AWS S3 bucket. Amazon S3 synchronously stores data across multiple facilities. Amazon S3 storage is designed to provide 99.999999999% durability of objects over a given year.
- Digital Commons Data ensures the integrity and authenticity of data deposited, by generating and verifying checksums for each file.
- Once a dataset version is published, and a DOI registered, the dataset version is immutable and permanently archived in a third party archival system, DANS (Data Archiving & Networked Services).

Preservation of deposited material:

- Published data is held permanently on Digital Commons Data; if an institutional Digital Commons Data repository ceases to operate, the institution's data will continue to be made available by Digital Commons Data.
- Furthermore, to ensure long-term preservation of data, all published datasets are stored with a third-party archive (DANS); which will ensure the data is available permanently at its registered DOI, even if Digital Commons Data were to cease operating.

Data curation:

- Digital Commons Data supports curation of datasets by institutional librarians and data stewards, by providing a pre-moderation capability, which allows institutional delegates to review every dataset prior to go-live, and either approve, make edits, or return the dataset to the author with comments to address before re-submitting. This allows liaising with depositors when issues are detected, before the dataset goes live.
- If issues are discovered with live datasets, then the institutional administrators may take the dataset down directly, as well as contacting the author offline.

Data security:

- Digital Commons Data has received ISO/IEC 27001:2013 certification in respect of secure information management practices.
- Digital Commons Data utilises secure interfaces such as TLS 1.2 or above. All data in transit and at rest is encrypted with at least AES-256 or equivalent. The repository supports secure encrypted data storage both on and offsite. It leverages AWS KMS tooling for secure key management.
- Digital Commons Data is hosted in AWS data centres. AWS has certification for compliance with ISO/IEC 27001:2013, 27017:2015, 27018:2019, and ISO/IEC 9001:2015.
- If authors wish to deposit sensitive data, the author may publish it within a Restricted-Access dataset: the files will be safely deposited, but cannot be accessed openly. Instead, researchers may request the files and the author can decide whether to release them.
- Elsevier has implemented a company-wide process for Business Continuity Management and Disaster Recovery with Recovery Point Objective and Recovery Time Objective windows congruent to our contractually agreed Service Level Agreements.
- Elsevier's Business Continuity Plan (BCP) is regularly audited, is in line with the international Business Continuity standards, and is ISO 22301 accredited.

Digital Commons Data offers information online in respect of its policies for acquisition and access to data, and its commitment to long-term preservation of data, on its [Mission page](), and in [FAQ]().