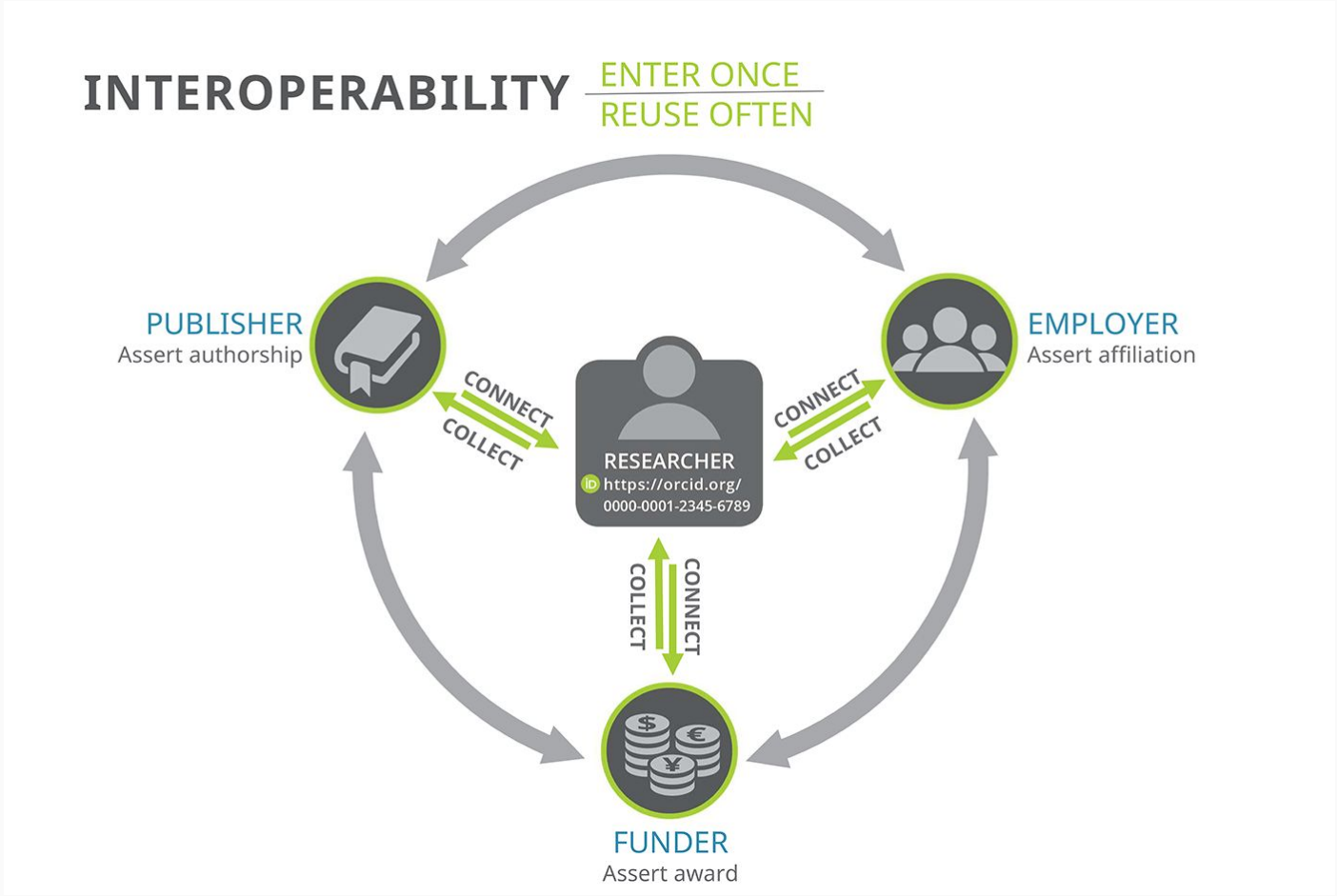
Visibility and privacy at ORCID

20th of October 2022

Paloma Marín-Arraiza, PhD, Engagement Manager Global Consortia

Researchers in the centre of what we do

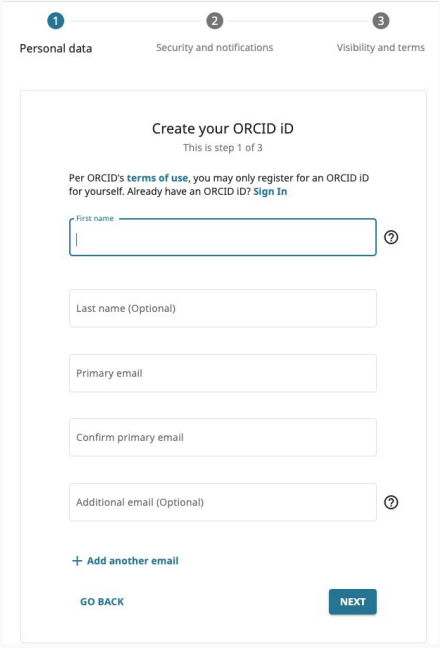


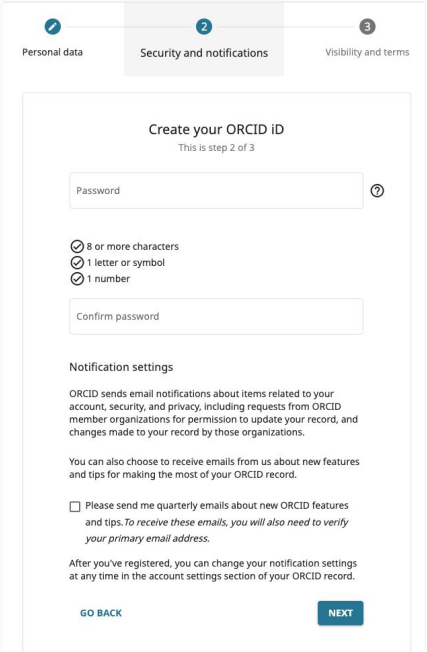
https://info.orcid.org/outreach-resources/

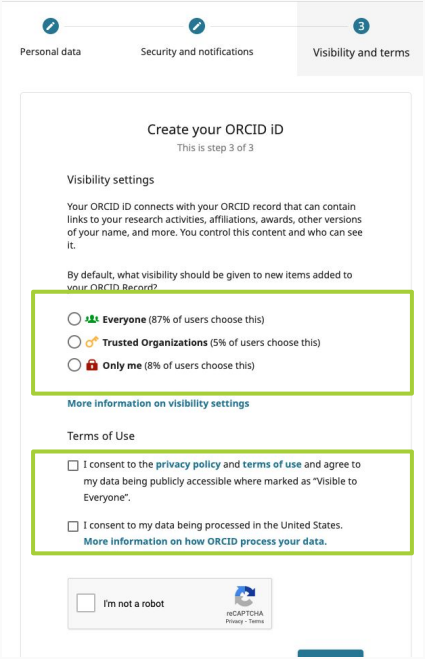
Visibility control, step by step

Visibility during the registration process

When users go to https://orcid.org/register



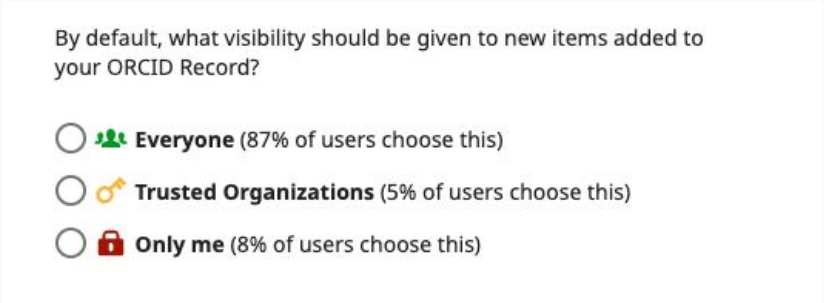




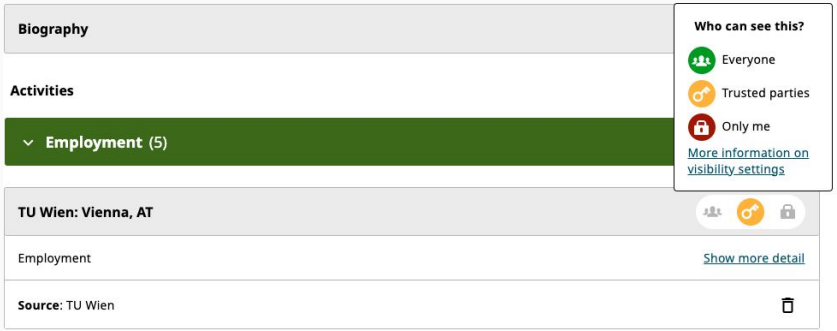
Further details: https://support.orcid.org/hc/en-us/articles/360006897614
Note: e-mail addresses are set to private by default

Visibility settings in detail

Default record visibility

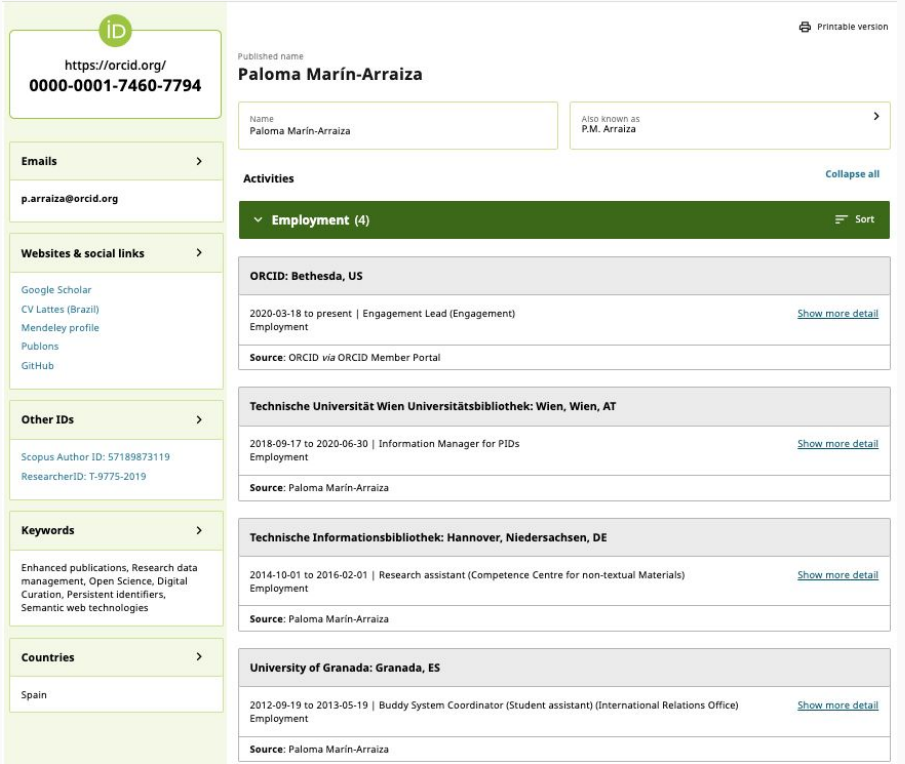


Individual item visibility

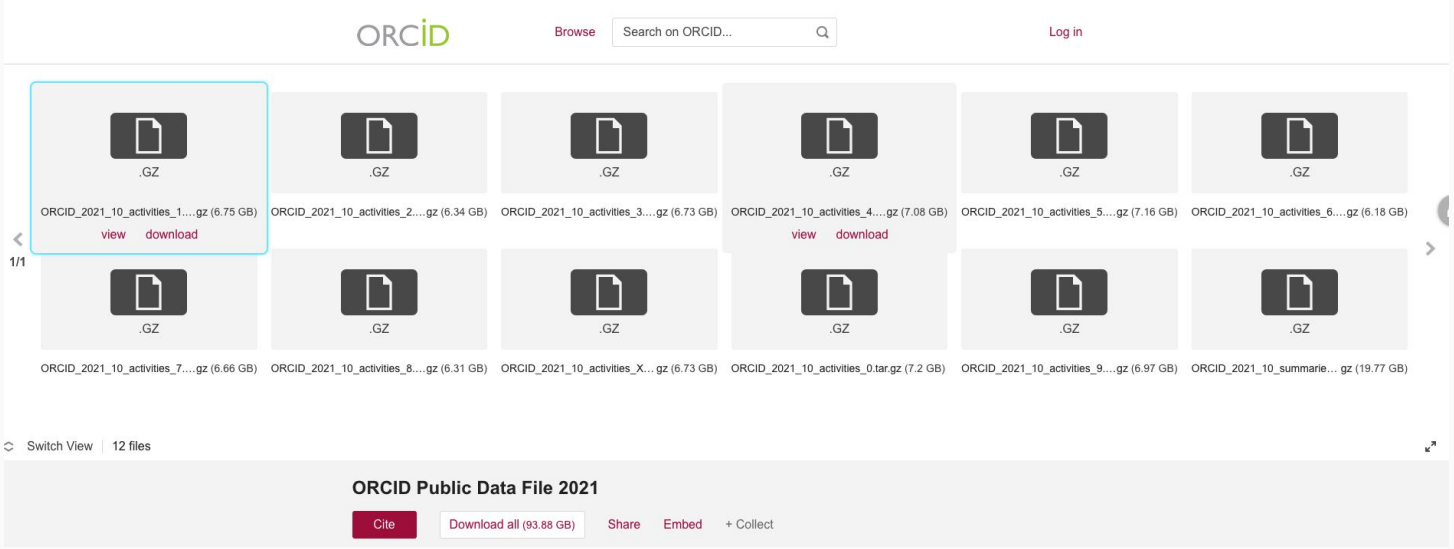


What does “Visible to everyone” mean?

- Visible in the ORCID record
- Available via the Public API (and also the Member API)
- Part of the Public Data File



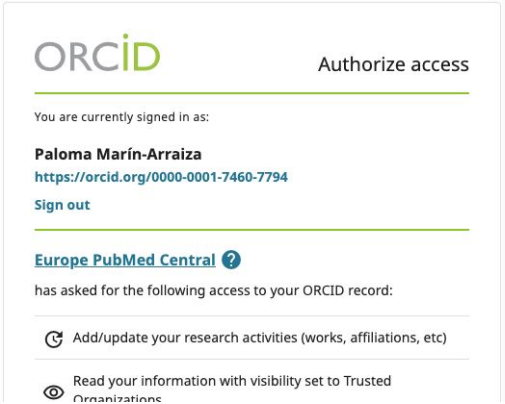
Public data on the ORCID Registry is open to all

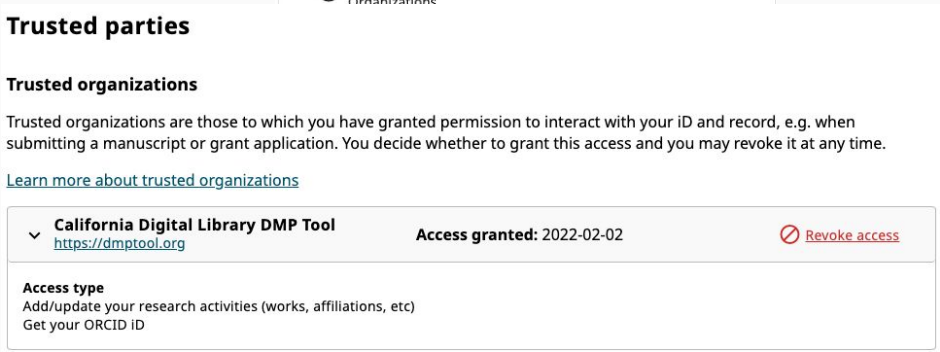


- ORCID Public Data File 2021: https://doi.org/10.23640/07243.16750535.v1
- XML to JSON - ORCID Conversion Library: https://github.com/ORCID/orcid-conversion-lib
- Public Data File use policy: https://info.orcid.org/public-data-file-use-policy/
- This file is provided to the public for research and statistical purposes and is available under a CC0 license.

What does “Visible to trusted parties” mean?

- When researchers connect their ORCID iD to another organization’s system, they will be asked to grant permission to that organization to interact with their ORCID account.
- Permissions are related with the API scopes and the actions that the organization is allowed to perform.
- Permissions can be revoked at any time





https://info.orcid.org/documentation/features/member-api/access-trusted-data/
https://support.orcid.org/hc/en-us/articles/360006973893-Trusted-organizations
https://curity.io/resources/learn/privacy-and-gdpr/

ORCID Privacy principles and GDPR individual rights

ORCID Privacy Principles

For researchers:

- You own your ORCID iD and record
- You control who accesses the information in your ORCID record
- You may change access preferences at any time
- You may close your ORCID account at any time
- Organizations may only add information to your ORCID record if you have granted permission for them to do so, and they may only update or remove information that was added by them

GDPR individual rights at ORCID

Right to data portability

Article 20 of the GDPR sets out your right to data portability – the right to have access to all your personal data in a common, machine-readable format. To access your data, use the Download your ORCID data feature in your Account settings to download all your personal data in XML format.

Right to access

Article 15 of the GDPR sets out your right to access – the right to learn from ORCID whether any of your personal data is being stored and processed.

Right to object

Article 21 of the GDPR sets out your right to object to the processing of data relating to yourself.

Right to erasure

Article 17 of the GDPR sets out your right to erasure – the right for any personal data concerning yourself to be erased. Sometimes referred to as the "right to be forgotten", this right includes the erasure of data added to your ORCID record by you or by any of your trusted individuals and organizations.

Right to rectify

Article 16 of the GDPR sets out your right to rectification – the right to edit any inaccurate personal data about you stored in the ORCID Registry.

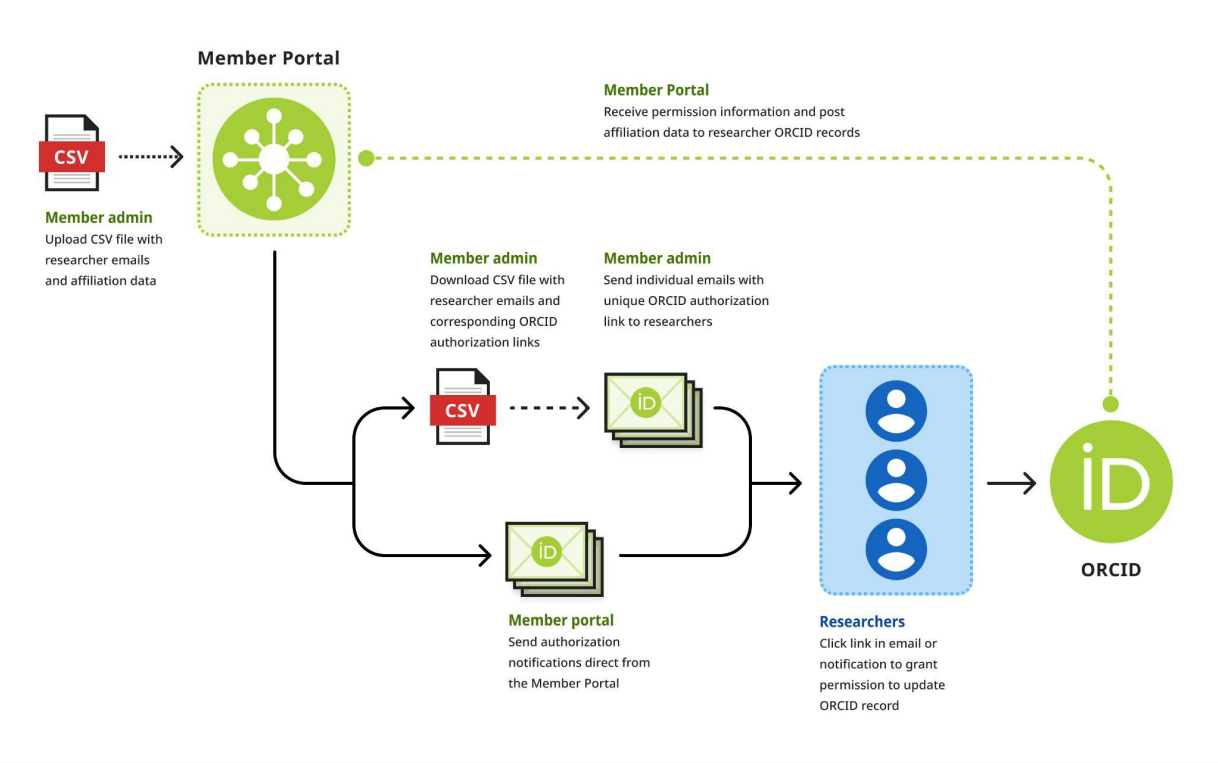
ORCID's dispute procedures.

GDPR Roles at ORCID

Roles and responsibilities

- **ORCID** → Controller (Registry) or Processor (Affiliation Manager)
- **Members** → Controller (Repository, HR System, CRIS System, Publishing system, Grant system…)
- **Researchers** → Data subjects
- Sub-processors for the registry
- Sub-processors for the member portal

ORCID as Processor in the Affiliation Manager



International data transfers

Safeguards for international data transfers

Context: ECJ Schrems II decision. In its decision, the ECJ raised concerns regarding whether personal data transferred from the EU to the US maintained adequate protection once stored within the US.

Analysis: External legal analysis to understand the impact.

Solution: Implementation of the EU Standard Contractual Clauses (SCCs).

Supplementary measures: Data subject control, Third-Party Processor Agreements, Data Encryption, Technical and Organizational Measures.

https://info.orcid.org/privacy-policy/#110_International_Data_Transfer
https://info.orcid.org/our-principles-policies/faq-orcid-and-ecj-schrems-ii-decision/
https://support.orcid.org/hc/en-us/articles/360006897574-ORCID-security

Thank you very much for attention
Děkujeme za pozornost

p.arraiza@orcid.org
Twitter: @pmarrai