Trust framework - Gaia-X Trust Framework - 22.04 Release

Table of Contents

1. Gaia-X Trust Framework

For Gaia-X to ensure a higher and unprecedented level of trust in digital platforms, we need to make trust an easy to understand and adopted principle. For this reason, Gaia-X developed a Trust Framework â€" formerly known as Gaia-X Compliance - and Labelling Framework that safeguards data protection, transparency, security, portability, and flexibility for the ecosystem as well as sovereignty and European Control.

The Trust Framework is the set of rules that define the minimum baseline to be part of the Gaia-X Ecosystem. Those rules ensure a common governance and the basic levels of interoperability across individual ecosystems while letting the users in full control of their choices.[1]

In other words, the Gaia-X Ecosystem is the virtual set of participants and service offerings following the Gaia-X requirements from the Gaia-X Trust Framework.
The Trust Framework uses verifiable credentials and linked data representation to build a FAIR knowledge graph of verifiable claims from which additional trust and composability indexes can be automatically computed.

The set of computable rules known as compliance process is automated and versionned. It means that this document will also be versionned.

1.1 Trust Framework scope

Those rules apply to all Gaia-X Self-Description files and there is a Self-Description files for all the entities defined as part of the Gaia-X Conceptual model described in the Gaia-X Architecture document:

This list mainly consists of:

- Participant with Consumer, Federator, Provider
- Service Offering
- Resource

1.1.1 Gaia-X Labels

The Labelling Framework itself is further detailed and translated into concrete criteria and measures in the Gaia-X Labelling Criteria document 22.04.

Framework	Notes
Trust Framework	Compulsory set of rules to comply with in other to be part of the Gaia-X Ecosystem. Individual ecosystems can extend those rules.

Framework	Notes
Labelling Framework	Optional set of criteria for Service Offerings.

1.2 Gaia-X Self-Description

Gaia-X Self-Description files are:

- machine readable text file
- cryptographically signed file preventing tampering with its content
- using link-data to describe attributes

The format is following the W3C Verifiable Credentials Data Model.

1.3 Gaia-X Trust Framework

There are 4 types of rules:

- serialization format and syntax.
- cryptographic signature validation and validation of the keypair associated identity.
- attribute value consistency.
- attribute veracity verification.

2. Trust anchors

For the compliance, Trust anchors are Gaia-X endorsed entities responsible to manage certificate to sign claims.

To be compliant with the Gaia-X Trust Framework, all keypairs used to sign claims must have at least one of the Trust Anchor in their certificate chain.

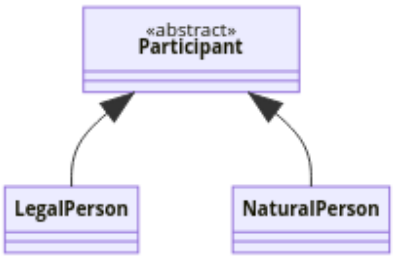
At any point in time, the list of valid Trust Anchors is stored in the Gaia-X Registry.

2.1 List of defined trust anchors

Name	Defined as
State	The Trust Service Providers (TSP) must be a state validated identity issuer. - For `participant`, if the `legalAddress.country` is in EEA, the TSP must be eiDAS compliant. - Until end of 2022 Q1, to ease the onboarding and adoption this framework DV SSL can also be used. - Gaia-X association is also a valid TSP for Gaia-X association members.
eiDAS	Issuers of Qualified Certificate for Electronic Signature as defined in eIDAS Regulation (EU) No 910/2014 (homepage: https://esignature.ec.europa.eu/efda/tl-browser/#/screen/home) (machine: https://ec.europa.eu/tools/lotl/eu-lotl.xml)
DV SSL	Domain Validated (DV) Secure Sockets Layer (SSL) certificate issuers are considered to be temporarily valid Trust Service Providers. (homepage: https://wiki.mozilla.org/CA/Included_Certificates) (machine: https://ccadb-public.secure.force.com/mozilla/IncludedCACertificateReportPEMCSV)
Gaia-X	*To be defined after 2022Q1.*
EDPB CoC	List of Monitoring Bodies accreditated to the Code of Conduct approved by the EDBP (list of EDBP's CoC: https://edpb.europa.eu/our-work-tools/documents/our-documents_fr?f%5B0%5D=all_publication_type%3A61&f%5B1%5D=all_topics%3A125)
gleif	List of registered LEI issuers. (homepage: https://www.gleif.org/en/about-lei/get-an-lei-find-lei-issuing-organizations) (machine: https://api.gleif.org/api/v1/registration-authorities)

3. Participant

A Participant is a Legal Person or Natural Person, which is identified, onboarded and has a Gaia-X Self-Description. Instances of Participant neither being a legal nor a natural person are prohibited.



Architecture Document defines three roles a Participant can have within the Gaia-X ecosystem (Provider, Consumer, and Federator), which are not yet part of Trust framework and are to be defined in future releases.

3.1 Legal person

For legal person the attributes are

Version	Attribute	Cardinality	Trust Anchor	Comment
1.0	`registrationNumber`	1	State	Country's registration number which identify one specific company.
1.0	`headquarterAddress` . `country`	1	State	Physical location of head quarter in ISO 3166-1 alpha2, alpha-3 or numeric format.
1.0	`legalAddress` . `country`	1	State	Physical location of legal registration in ISO 3166-1 alpha2, alpha-3 or numeric format.
1.0	`leiCode`	0..1	gleif	

Version	Attribute	Cardinality	Trust Anchor	Comment
				Unique LEI number as defined by https://www.gleif.org.
1.0	`parentOrganisation[]`	0..*	State	A list of direct `participant` that this entity is a subOrganization of, if any.
1.0	`subOrganisation[]`	0..*	State	A list of direct `participant` with an legal mandate on this entity, e.g., as a subsidiary.

Consistency rules

- If `legalAddress.country` is located in European Economic Area, Iceland, Lichtenstein and Norway then `registrationNumber` must be a valid ISO 6523 EUID as specified in the section 8 of the Commission Implementing Regulation (EU) 2015/884.
  This number can be found via the EU Business registers portal
- If `legalAddress.country` is located in United States of America, than a valid `legalAddress.state` using the two-letter state abbreviations is mandatory
- `leiCode.headquarter.country` shall equal `headquarterAddress.country`.
- `leiCode.legal.country` shall equal `legalAddress.country`.

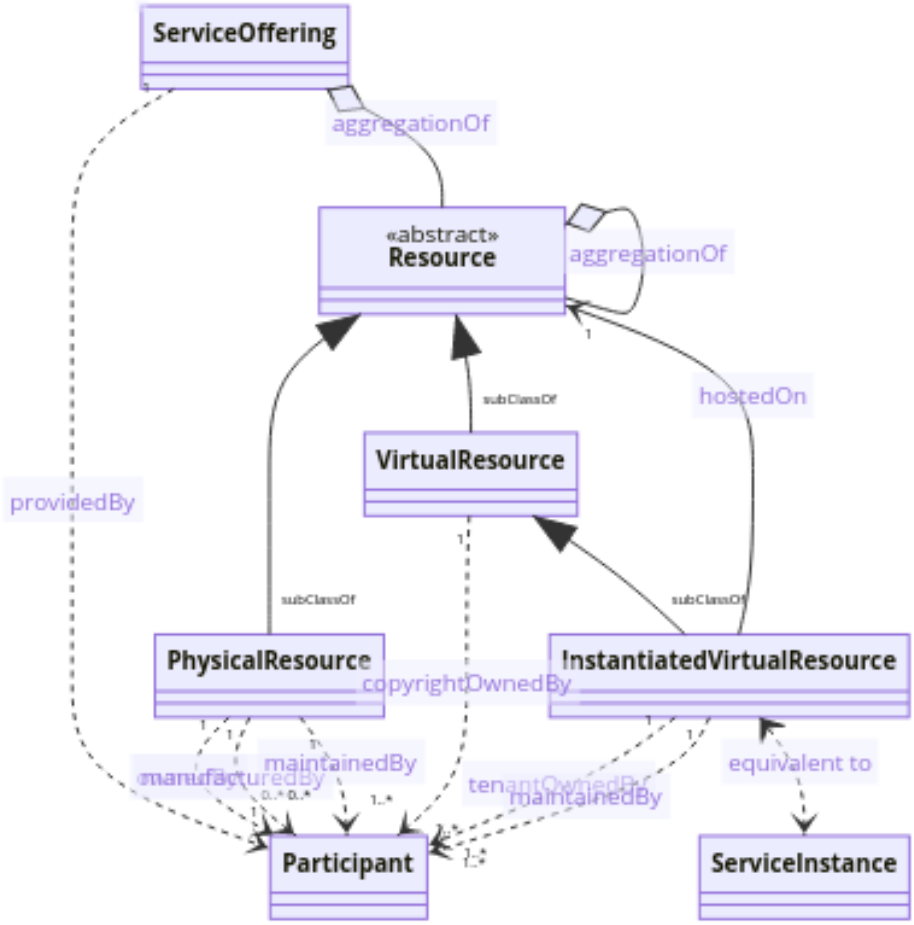
3.2 Natural person

To be defined in a future release.

4. Services & Resources

Here is the main model for service composition, also included in the Gaia-X Architecture document.

A `Service Offering` can be associated with other `Service Offerings`.



4.1 Service offering

This is the generic format for all service offerings

Version	Attribute	Card.	Trust Anchor	Comment
1.0	`providedBy`	1	State	a resolvable link to the `participant` self-description providing the service

Version	Attribute	Card.	Trust Anchor	Comment
1.0	`aggregationOf[]`	0..*	State	a resolvable link to the `resources` self-description related to the service and that can exist independently of it.
1.0	`termsAndConditions[]`	1..*	State	a resolvable link to the Terms and Conditions appling to that service.
1.1	`policies[]`	0..*	State	a list of `policy` expressed using a DSL (e.g., Rego or ODRL)
1.x	`gdpr`	0..1	*see below*	Specific attributes for the General Data Protection Regulation.
1.x	`lgpd`	0..1	*see below*	Specific attributes for the General Personal Data Protection Law. (*Lei Geral de Protecao de Dados Pessoais*)
1.x	`pdpa`	0..1	*see below*	Specific attributes for the Personal Data Protection Act 2012.

TermsAndConditions structure

Version	Attribute	Card.	Trust Anchor	Comment
1.0	`URL`	1	State	a resolvable link to document
1.0	`hash`	1	State	sha256 hash of the above document.

Consistency rules

- `gdpr` attributes are mandatory when the service is provided in EEA or when the `providedBy` participant is located in EEA.
- `lgpd` attributes are mandatory when the service is provided in Brazil or when the `providedBy` participant is located in Brazil.
- `pdpa` attributes are mandatory when the service is provided in Singapore or when the `providedBy` participant is located in Singapore.

4.1.1 GDPR

Version	Attribute	Card.	Trust Anchor	Comment
x.x	`to_be_defined`	1	State, EDPB CoC	mandatory public information as defined in GDPR

4.1.2 LDPR

Version	Attribute	Card.	Trust Anchor	Comment
x.x	`to_be_defined`	1	to be defined	mandatory public information as defined in LDPR

4.1.3 PDPA

Version	Attribute	Card.	Trust Anchor	Comment
x.x	`to_be_defined`	1	to be defined	mandatory public information as defined in PDPA

Addition specific criteria per Service Offering are described in the next section.

4.2 Resource

A resource aggregates with Service Offering.

Version	Attribute	Card.	Trust Anchor	Comment
1.0	`aggregationOf[]`	0..*	State	`resources` related to the resource and that can exist independently of it.

4.2.1 Physical Resource

A Physical Resouce inherits from a Resource.
A Physical resource is, and not limited to, a datacenter, a baremetal service, a warehouse, a plant. Those are entities that have a weigth and position in our space.

Version	Attribute	Card.	Trust Anchor	Comment
1.0	`maintainedBy[]`	1..*	State	a list of `participant` maintaining the resource in operational condition and thus have physical access to it.
1.0	`ownedBy[]`	0..*	State	a list of `participant` owning the resource.
1.0	`manufacturedBy[]`	0..*	State	a list of `participant` manufacturing the resource.
1.0	`locationAddress[].country`	1..*	State	a list of physical location in ISO 3166-1 alpha2, alpha-3 or numeric format.
1.0	`location[].gps`	0..*	State	a list of physical GPS in ISO 6709:2008/Cor 1:2009 format.

4.2.2 Virtual Resource

A Virtual Resource inherits from a Resource.
A Virtual resource is a resource describing recorded information such as, and not limited to, a dataset, a software, a configuration file, an AI model.

Version	Attribute	Card.	Trust Anchor	Comment
1.0	`copyrightOwnedBy[]`	1..*	State	A list of copyright owner either as a free form string or `participant` self-description. A copyright owner is a person or organization, that has the right to exploit the resource. Copyright owner does not necessary refer to the author of the

Version	Attribute	Card.	Trust Anchor	Comment
				resource, who is a natural person and may differ from copyright owner.
1.0	`license[]`	1..*	State	A list of SPDX license identifiers or URL to license document

4.2.3 Instantiated Virtual Resource

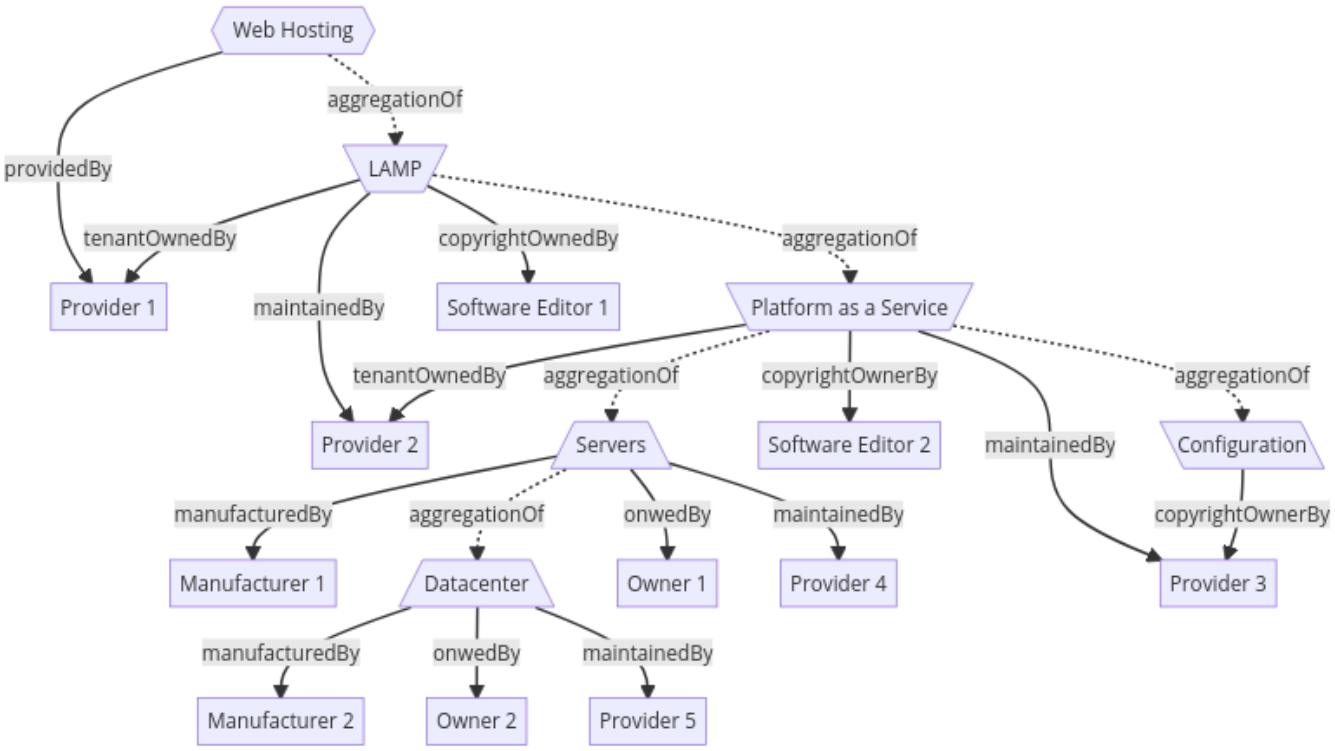
An Instantiated Virtual Resource inherits from a Virtual Resource.
An Instantiated Virtual resource is a running resource exposing endpoints such as, and not limited to, a running process, an online API, a network connection, a virtual machine, a container, an operating system.

Version	Attribute	Card.	Trust Anchor	Comment
1.0	`maintainedBy[]`	1..*	State	a list of `participant` maintaining the resource in operational condition.
1.0	`hostedOn`	1	State	a `resource` where the process is running, being executed on.
1.0	`tenantOwnedBy[]`	1..*	State	a list of `participant` with contractual relation with the resource.
1.x	`endpoint[]`	1..*	State	a list of exposed endpoints as defined in ISO/IEC TR 23188:2020

5. Examples

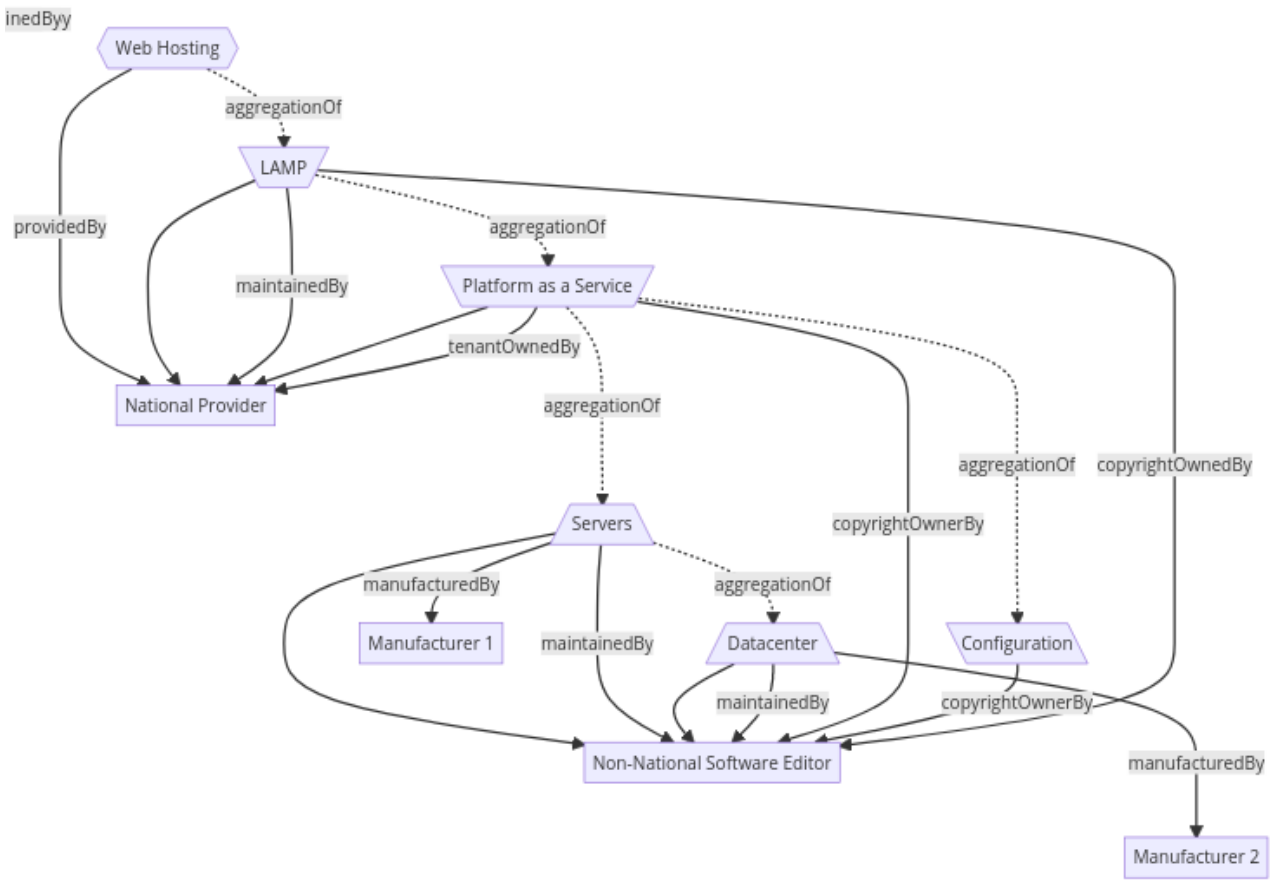
5.1 Generic LAMP offering

LAMP is an acronym for Linux, Apache, MySQL, PHP. It is a software stack consisting of the operating system, an HTTP server, a database management system and an interpreted programming language, and is used to set up a web server.



5.1.1 LAMP offering using one software vendor

Example of a LAMP offering with one software vendor.
This diagram can be used to illustrate how several "Trusted Cloud" offers are built.

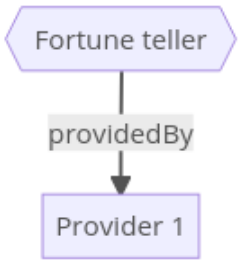


5.2 Simple Fortune teller

Example of a simple API endpoint returning a fortune from the BSD packet fortune.

For the same service offering, 3 examples of service offering are detailled with 3 different transparency level: Trust_Index(Service Offering 1 v1.0) < Trust_Index(Service Offering 1 v2.0) < Trust_Index(Service Offering 1 v3.0)

5.2.1 Fortune teller v1.0



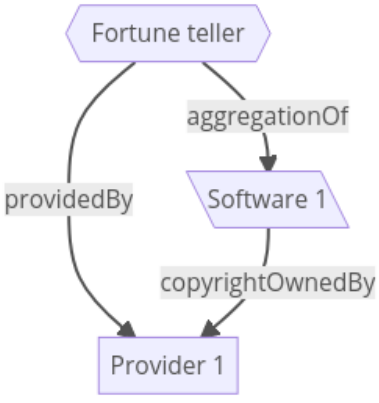
Service Offering

```
name: Fortune teller
description: API to randomly return a fortune
providedBy: url(provider1)
termsAndConditions:
  - https://some.url.for.terms.and.condition.example.com
```

Provider 1

```
registrationNumber: FR5910.899103360
headquarterAddress:
  country: FR
legalAddress:
  country: FR
```

5.2.2 Fortune teller v2.0



Service Offering

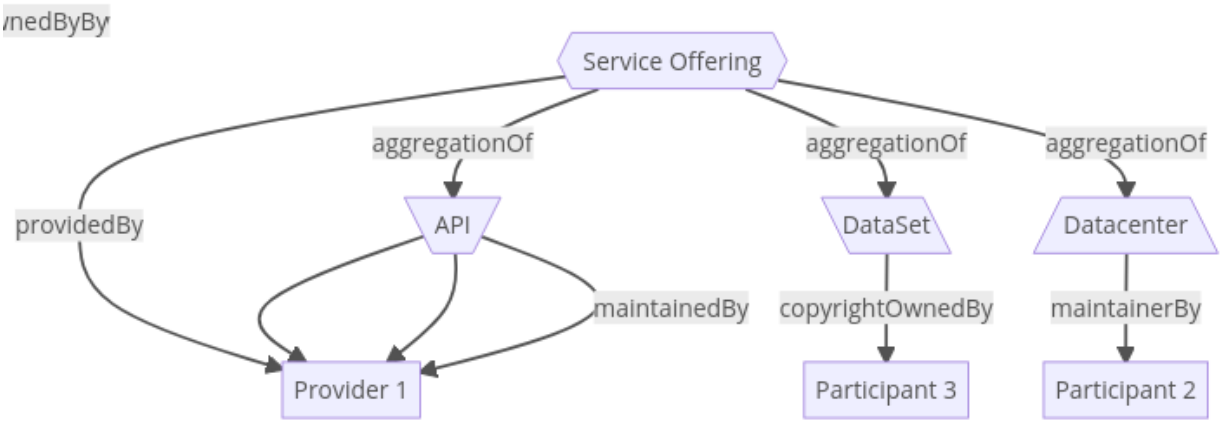
```
name: Fortune teller
description: API to randomly return a fortune
providedBy: url(provider1)
```

```
aggregationOf:
  - url(software1)
termsAndConditions:
  - https://some.url.for.terms.and.condition.example.com
```

Software 1

```
name: api software
copyrightOwnedBy:
  - url(provider1)
license:
  - EPL-2.0
```

5.2.3 Fortune teller v3.0



Service Offering

```
name: Fortune teller
description: API to randomly return a fortune
providedBy: url(provider1)
aggregationOf:
  - url(software1)
  - url(dataset1)
  - url(datacenter1)
termsAndConditions:
  - https://some.url.for.terms.and.condition.example.com
policies:
  - type: opa
    content: |-
      package fortune
      allow = true {
```

```
      input.method = "GET"
    }
```

API 1

```
name: api software
maintainedBy:
  - url(provider1)
tenantOwnedByBy:
  - url(provider1)
copyrightOwnedBy:
  - url(provider1)
license:
  - EPL-2.0
```

Dataset 1

```
name: fortune dataset
copyrightOwnedBy:
  - name: The Regents of the University of California
    registrationNumber: C0008116
    headquarterAddress:
      state: CA
      country: USA
    legalAddress:
      state: CA
      country: USA
license:
  - BSD-3
  - https://metadata.ftp-master.debian.org/changelogs//main/f/fortune-mod/fortune-mod_1.99.1-7.1_copy
```

Participant 2

```
name: Cloud Service Provider
registrationNumber: FR5910.424761419
headquarterAddress:
  country: FR
legalAddress:
  country: FR
```

Datacenter 1

```
name: datacenter
maintainedBy: url(participant2)
location:
 - country: FR
```

---

1. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf ↩