**Roles, technical requirements and guiding principles**

|  |  |  |
| --- | --- | --- |
| **Actor** | **Technical requirement** | **Guiding principles & notes** |
| The role of an **Identity Authority** (IDA) is to oversee the effective, open running of the eco-system and to administer the operation of the IDA service. The IDA service issues and checks unique pseudonymous keys that provide security and ensure the interoperability and universality of the ecosystem. |
| **Identity Authority** | shall | Maintain an always-on IDA service that will return or validate unique pseudonymous keys to Data Engine, Service Provider & Operator | P4 |
| Be a non-profit legal entity | P5 |
| Provide its services on a fair, reasonable and non-discriminatory basis | P5 |
| Provide Consumers with information about the operation of the eco-system free of charge | P5 & P7 |
|  |  |
| shall not | Act as a Data Engine or Service Provider (other than for the purposes of providing a limited ‘sandbox’ test environment) | P4 & P5 |
| Store Behavioural Atoms | P4 & P5 |
| Hold any Consumer’s directly identifying personal information (DIPI) | P5 |
|  |  |
| may | Request Data Engine support to deliver population-level insights for public information and the purposes of marketing the specification | P6 |
| Make a query on Data Engines to ensure a specific ConsumerID has been forgotten | P7This allows the Identity Authority to audit the forgetting process. |
| Provide Consumers with information about their status within the eco-system | P5 & P7 |
| Provide audit services to Data Engine, Service Provider, Operator and regulators | P6 |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Actor** | **Technical requirement** | **Guiding principles & notes** |
| The role of the **Data Engine** is to receive, store and process Behavioural Atoms. Data Engines provide business-to-business services to Service Providers and other organisations in the form of queries that create Report Data. |
| **Data Engine** | shall | Provide secure storage of Behavioural Atoms for a period to be agreed with the Service Provider in line with the Consumer consent | P2 & P3 |
| Provide minimal interface services for Service Providers to process joiners, movers, and leavers (e.g. Operator & Consumer trees, registration, ID re-allocation, forgetting) | P4 |
| Provide minimal interface services for querying Behavioural Atoms by registered Service Providers | P1 |
| Maintain an always-on, single entry point for uploading Behavioural Atoms to the Data Engine | P4 |
| Receive Behavioural Atoms from Consumers or Devices registered with their Operators that conform to the specification free of charge | Receiving data is a minimal requirement for a Data Engine, commercial services apply to the use and processing of data. |
| Ensure that their Service Providers have the minimum standard consent from Consumers | P3 |
| Notify Service Providers if they believe that their store of Behavioural Atoms contains DIPI | P1 & P6 |
| Provide information to the Service Provider about the location and security of the infrastructure used in the delivery of services | P7 |
| Notify Service Providers any mergers and acquisitions or other changes that would result in a change of control of the data store | P7 |
| Check the credentials of a Service Provider every time a request is made to release data for a ConsumerID  | Security. |
| Provide an additional security check when Service Providers request Consumers to be forgotten to reduce the risk of unauthorised data loss. | Security. |
|  |  |
| shall not | Link Behavioural Atom data to directly-identifying personal information (DIPI) from external sources | P1 |
| Link Behavioural Atom data directly to external data storage if such link might directly identify Consumers | P1 |
| Hold any Consumer’s directly identifying personal information (DIPI) | P1 |
| Act as a Service Provider or Operator itself | P1 & P4 |
| Request more than the Segment Data as defined in the specification (gender, year of birth, time zone & latitude to 0 decimal points) on registration of a Consumer  | P1 |
| Knowingly receive DIPI | P1 |
| Levy unreasonably punitive charges for the complete download of store of Behavioural Atoms | Supports EU data protection and an open, competitive eco-system. |
| Utilise IDA unique pseudonymous keys outside of the ecosystem | P1 |
|  |  |
| may | Add non-personal data to the atom store to deliver enhanced services (e.g. local weather data) | P1While Behavioural Atoms should not be linked out, additional information can be linked in. |
| Use suitable aggregation techniques rendering the data non-personal to provide indirect services to other parties | P1 & P6 |
| Host multiple Service Providers |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Actor** | **Technical requirement** | **Guiding principles & notes** |
| **Service Providers** are the primary link between a Consumer and a Data Engine. They are able to query the atoms held by a Data Engine to develop personalised services for Consumers based on their everyday behaviours. Service Providers will often be consumer facing brands. |
| **Service Provider** | shall | Ensure that their Operators have the minimum standard consent from Consumers | P3 |
| Secure additional consent from Consumers when sending personal information outside the eco-system | P3 & P6 |
| When sending Behavioural Atom information outside the eco-system, remove the ConsumerID and replace with DIPI | P6This ensures that information that has left the eco-system can be clearly identified. |
| Ensure that their Operators follow the specification | P6 |
| For any one purpose and at any one time, have only one Data Engine | Avoids potential data loss for the consumer and ensure the complete audit map of the eco-system. |
| On a request from a Consumer, supply all DIPI, Segment Data, Behavioural Atoms and any stored Report Data | P2Basic tenet of EU data protection. |
| On a request from a Consumer to be forgotten, remove or render DIPI to be non-personal | Basic tenet of EU data protection. |
| On a request from a Consumer to be forgotten, instruct their Data Engine remove or render data to be non-personal | P2 & P3 |
| On a request from an Operator or Consumer, provide the identity of the Data Engine | P7 |
| Notify Consumers (via Operators) of any mergers and acquisitions or other changes that would result in a change of control over the Consumers’ data | P7 |
| Check the credentials of an Operator every time a request is made to release data for a ConsumerID  | Security. |
| Ensure that all Operators within a specific embodiment are working under equivalent terms (e.g. consent, purpose, retention periods etc). | P7 |
| Use different passwords to interact with different actors in the ecosystem (within the same service embodiment). | Security. |
| Use a different ServiceProviderID for every instance of a service embodiment in which they are an actor | Security. |
|  |  |
| shall not | Receive Behavioural Atoms directly | P1 |
| Send DIPI to a Data Engine | P1 |
| Share DIPI or Behavioural Data with another Service Provider without additional informed consent from the Consumer  | P3 |
| Utilise IDA unique pseudonymous keys outside of the ecosystem | P1  |
|  |  |
| may | Transfer its operations between Data Engines | Supports open, competitive eco-system. |
| Host multiple Operators |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Actor** | **Technical requirement** | **Guiding principles & notes** |
| The **Operator** is the entity that administers the contact with the Consumer. It holds the directly-identifying personal information (DIPI) required to engage with the Consumer. An Operator may be an independent app, exist within a Service Provider or be an independent organisation. Operators only receive information from their Consumers and their Service Provider. |
| **Operator** | shall | Provide a mechanism for the consumer to access their ConsumerID | This allows the Identity Authority to audit the ‘forgetting’ process. |
| Ensure that the minimum standard consent is given by Consumers - freely, specific & informed | P3 |
| For any one purpose and at any one time, have only one Service Provider | Avoids potential data loss for the consumer and ensure the complete audit map of the eco-system. |
| Clearly identify the Service Provider to the Consumer | P7 |
| Notify Consumers of any mergers and acquisitions or other changes that would result in a change of control over the Consumers’ data | P7 |
| Hold ConsumerID pseudonymous keys with the same security level as DIPI | Security |
| Use different passwords to interact with different actors in the ecosystem (within the same service embodiment). | Security. |
| Use a different ServiceProviderID for every instance of a service embodiment in which they are an actor | Security. |
|  |  |
| shall not | Store Behavioural Atoms other than for the purposes of transmission to the Data Engine.  | P1 |
| Send DIPI to a Data Engine | P1 |
| Share DIPI with another Operator or Service Provider without additional consent from the Consumer  | P3 |
| Utilise IDA unique pseudonymous keys outside of the ecosystem | P1 |
|  |  |
| may | Host multiple Consumers |  |
|  |  |

|  |  |  |
| --- | --- | --- |
| **Actor** | **Technical requirement** | **Guiding principles & notes** |
| The **Consumer** is the generic reference to any individual registered with the eco-system. They may be patients in a healthcare setting, subjects in a trial as well as consumers of a commercial digital service. A Consumer’s primary relationship may be with a Service Provider via a near-invisible Operator or with clearly recognisable Operator that is supported by a Service Provider in the background. |
| **Consumer** | shall |  |  |
|  |  |
| shall not |  |  |
|  |  |
| may | Request to be ‘forgotten’ in the eco-system | Basic tenet of EU data protection. |
| Request the Identity Authority to audit their status in the eco-system | P5 & P7 |
| Request the Operator to supply their DIPI, Segment Data, Behavioural Atoms and any stored Report Data | Basic tenet of EU data protection. |
|  |  |

**Principles**

**P1 Data Separation Principle**

The specification implements a separation of data types: Data engines keep data on *what* you do (Behavioural Atoms) and the Service Provider/Operator keeps data on *who* you are (DIPI). No single organisation holds both sets of data together. This means that it would need a double accidental or malicious disclosure for connected information to be released.

**P2 Data Atomisation Principle**

Data is deliberately broken down into a small chunk of information by the Operator and coded with their ConsumerID (which implies their atomised consent) – each separate Behavioural Atom has a very low privacy risk. Neither the Operator/Service Provider sees these atoms as raw atoms and can only see composite data from Data Engine under the terms of the specification.

**P3 Atomised Consent Principle**

Consumer gives informed consent to the Operator under guideline terms set by the specification. Consent allows the Operator to sign up the consumer with a ConsumerID. This ConsumerID is the indicator to Identity Authority and other eco-system actors that the consumer has given appropriate consent. Because each and every Behavioural Atom has the ConsumerID, each atom has that consumers consent written into the structure of the data. Removing the ConsumerID from a Behavioural Atom is removing the consent of that individual so the data can no longer be used by either the Operator/Service Provider who signed them up. Now the Behavioural Atom is marked as an Anon-ConsumerID atom. Rules applied to these Behavioural Atoms by the Data Engine are different depending on the un-consent from the consumer. The time stamp uniquely associated with each Behavioural Atom allows full auditing of this principle.

**P4 Separation of Competence Principle**

Data Engines are expert data handlers. They know how to run robust, secure and always on cloud based data services; they handle Behavioural Atoms NOT Consumers. Service Providers / Operators are experts at Consumer facing / relevant services and handling DIPI; they handle Consumers NOT Behavioural Atoms. The Identity Authority is expert at overseeing the ecosystem.

**P5 No Conflict of Interest Principle**

Consumers need to see that there are no conflicts around their data. To ensure this, the Identity Authority acts on behalf of the Consumer in partnership with Operator/Service Provider, Data Engine and regulators.

 **P6 Active support Principle**

All actors will actively promote the principles of the specification, safeguard the structure of the eco-system and support good data practice for both consumers and enterprise.

**P7 Transparency Principle**

The roles and identities of all the actors in the eco-system who are working together on behalf of a Consumer should be clear and visible to that Consumer.

**Glossary & Nomenclature**

**Directly Identifying Personal Information (DIPI)**

Static or slow-changing data required to provide services to a Consumer including, for example: name, date of birth, contact information, medical/insurance numbers, payment details, etc. Specifically excluding all event-based information (Behavioural Data / Atoms). This is information that would be generally known as PII in a USA context.

**Segment Data**

Year of birth, gender, home time zone (GMT+/-x) and home latitude to single degree resolution.

**Behavioural Data**

Data that is coded according to the COEL TC protocols with, as a minimum, a Classification of Everyday Living code, a unique Consumer ID and a timestamp. A single instance is known as an Atom or Behavioural Atom.

**Report Data**

Data developed from the analysis of Behavioural Data (Atoms) for the purposes of developing insight and information for the provision of value-add services.

**Aggregated and anonymised summary data**

Data developed from the analysis of Behavioural Data (Atoms) for the purposes of comparison with Report Data and to deliver business to business services outside the Coelition ecosystem.

**ConsumerID**  An IDA unique pseudonymous key for a particular Consumer.

**Anon-ConsumerID** An IDA unique pseudonymous key for a forgotten Consumer.

**ServiceProvider.ID** An IDA unique pseudonymous key for a particular Service Provider.

**Operator.ID** An IDA unique pseudonymous key for a particular Operator.

**Device.ID** An IDA unique pseudonymous key for a particular consumer device.