Trust Frameworks for Data Sharing

Effective data mining requires enormous amounts of data, but not all organisations are data rich

Creating a Trust Framework to safely and securely share data with other organisations could significantly enhance your organisation's ability to benefit from data mining

tessellate

Technological advancement in business

Bird & Bird

Could your organisation benefit from creating a Trust Framework?

If any of these apply to you, read on to find out how you can create a Trust Framework

We have lots of data and want to share it safely in order to:

- experiment and explore what more it can tell us, and/or
- enhance and improve it

We need access to a bigger or different set of data in order to:

- enhance our products or services,
- market them more effectively, and/or
- be able to compete effectiviely with companies that have more data than us

We have identified a data tool that will enable us to effectively mine a large pool of data to achieve our desired outcomes but:

- we can't justify the CAPEX of the data tool on our own; and/or
- we don't have enough data for the tool to be truly effective

We have identified a potential partner whose data would be useful to us, we could each benefit from each other's data if there was a safe way to share it

What to consider when choosing data sharing partners

You've identified that your company could benefit from creating a Trust Framework. There are a number of practical issues to consider before deciding if they are the right partner for your business.

Commercial / Financial

1. **Value analysis: participation v status quo**
   - what does the organisation currently use data for, and what is the optimum result from data sharing?
   - asset-based vs open source approach
   - participation of competitors
   - quantification
2. **Limited individual data sets vs numerous sets**
   - scope of data provided
   - integrity and variety
   - unwanted bias
3. **Purpose of data sharing**
   - what are participants permitted and restricted from doing?
   - costs of establishment, maintenance and winding-up - how are these calculated and borne?
4. **Input data**
   - expected/required standards and volume
   - calculation basis
5. **Insurance**
   - how will it affect existing insurance, what new arrangements will be needed?

Operational / Technical

1. **Data input and metadata**
   - how will the data be ingested?
   - what metadata is required?
   - what format does it need to be in?
2. **Platform and data storage**
   - how will it be managed, who is responsible?
   - will it be run by a neutral third party?
3. **Process for data analysis**
   - what process will be used, who is responsible for it?
   - will you only share the input data, or will you also be sharing the outcomes of the analysis?
4. **Security**
   - how will the data pool be kept secure and who is responsible for security?

Ethical

1. **Anonymisation of data**
   - can/will the data be anonymised before being shared?
   - will the derived data be anonymous?
2. **Ensuring ongoing public/customer trust in process**
   - how will this be achieved?
   - what will happen if public/customer trust is compromised?
3. **Level of transparency to public/customers**
   - to what extent will customers be aware of the trust framework?
4. **Privacy/confidentiality**
   - beyond the parties' legal obligations, what other privacy/ confidentiality considerations are there?
   - likely to depend on the type of data to be shared
5. **Control**
   - have the parties properly screened the other members of the trust framework? Are they comfortable that they are suitable parties to take control of their customers' data?

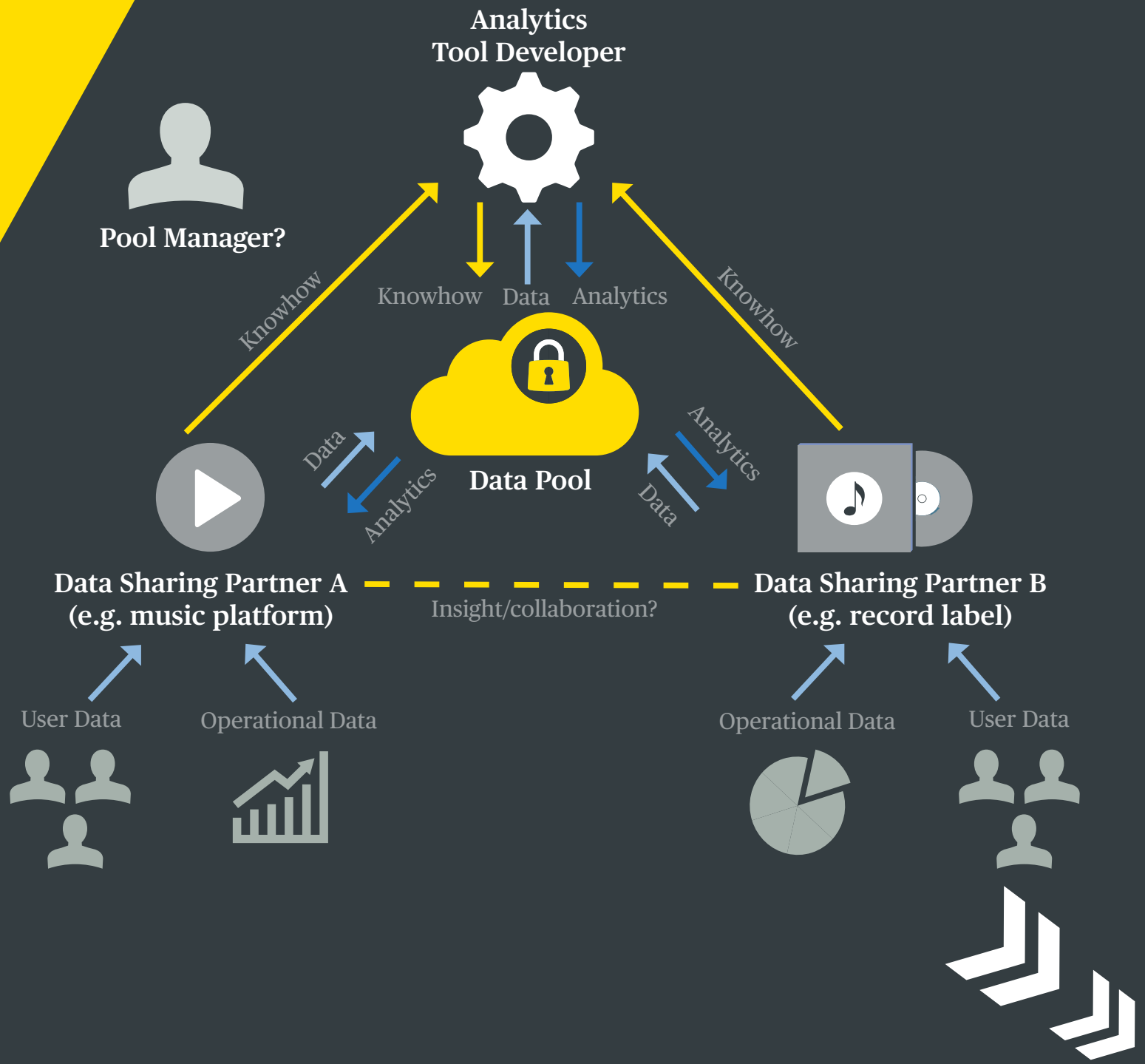
Legal

1. **Scope of obligations: must be clearly defined**
   - are the parties signing up to minimum quality/ volume commitments?
   - are there circumstances in which a participant could withhold data?
2. **Scope of use: must be clearly defined**
   - how restrictive should this be?
   - how much flexibility will the parties have to adapt to change of use cases?
3. **Governance – how are breaches policed and managed?**
   - what remedies are available if a party fails to provide sufficient quantity/quality data or misuses data?
   - how are security risks managed?
   - Liability for breaches
4. **End of Term**
   - what should happen to the input data and derived data following termination of the agreement/withdrawal of one or more parties?
5. **Competition law risks**
   - what are they and how can they be managed?
   - particularly relevant where sharing data with competitors or restricting parties' use of input/ derived data
6. **Audit rights**
   - how much do the parties trust each other?
   - how much scrutiny is required?

What could my Trust Framework look like?

Now that you have selected your data sharing partners, you will need to consider how to structure your Trust Framework.

For instance, it could look a bit like this...



How to build a Trust Framework

You've decided who to include within your Trust Framework. Now you need to put the appropriate agreements in place to ensure that the data can be shared and analysed safely and securely and in a way that achieves each party's desired outcomes. This raises some difficult legal considerations. Some of these are outlined below.

Technology procurement

- Off the shelf or bespoke technology solution?
- Are vendor lock-ins required?
- Will each party procure its own technology to run its own analytics or will the analytics be performed jointly?
- Confidentiality

Cyber Security

- Parties' secure obligations
- Apportionment of liability for data loss or breaches
- Management of the data pool - would it be useful to use a neutral third party to manage the data?
- Is it likely that there will be regular interference?
- Will or could the pool be made publicly available?

Ownership and control

Ownership and control of (a) input data, (b) the data pool and (c) derived data will be impacted by:

- IP clauses
- Audit rights
- Restrictions on the use and reuse of data
- Confidentiality

Data privacy

- Transparency of processing
- Role of the parties and basis for sharing data
- Lawfulness of processing
- Risks related to data scrapping (if relevant)
- Risks related to processing that involves any significant automated decision making
- Accountability requirements and impact assessments

Assessing the quality of your Trust Framework before committing to it

Data is a precious commodity and choosing to share it and allow others to mine it is a decision that should not be taken lightly. Of course, you can never know with complete certainly that you are making the right decision, but there are ways of testing the quality of your decision making.

The 6 Dimensions of Decision Making

Frame	Options	Information	Measures	Logic	Commitments
The context and background against which the technology is being implemented	The choices open to us about whether or how to implement the technology	The information available to me on which I can base my assessment of the options	The metrics by which I can assess the technology implementation – e.g. 'fail', 'acceptable', 'target'	The extent to which I can evaluate which options will create greatest value (against my measures)	The extent to which I can be confident I can deliver the chosen option

Technological advancement in business

Click here to register your interest in workshops/webinars relating to Data Mining and Trust Frameworks

Bird & Bird