Data Product Factory (DPF)

This document provides an overview of the DPF. It is targeted at an executive audience with an understanding of information technology, awareness of information security, privacy and it's meaning in the context of an individual i.e., a customer's view of participating with the digital world and internet.

The document provides background about complexities that organisations both private and public service or state actors (organisations) face and the impact that these challenges may have on the collection, protection and use of information held by an organisation.

The DPF is a software concept with the single goal in mind; enable organisations to deal with the impact of change on customer data for organisations. The document provides the background, insight and opportunity that has led to the development of the concept into a detailed design which can be developed into a software-as-a-service solution.

Document Purpose

The purpose of this document is to seek funding and support for the development of the Data Product Factory (DPF).

The document explains the following:

- Value proposition of the DPF for organizations and their customers.
- What problem(s) the DPF solve.
- How the DPF solves the problem.
- What gives the DPF a competitive edge.
- Industry Background

Contents

Value Proposition

All private-, public service or state owner organisations value customer information, whether it is the personal identifiable information, historical information, confidential information about health or finance. It is paramount to protect the information at all costs for the benefit of customers and self-preservation in that, information in the hands of a malicious actor could snuff competitors, spread fake political views and de-stabilize organisations or countries.

Information stand juxtaposed to its name, information is meant to is to 'inform', it must inform a courier where the delivery address is but at the same time shouldn't disclose information about parcel contents and even the information access rules must be protected to avoid identity impersonation.

The information landscape is a complex balancing act between granting and restricting access. In addition to information's innate complexity, an ever-changing technology and global connectedness of the internet means information protection controls must withstand internal change and external threats that operate at a global scale.

The DPF provides business value by:

1. **Building Customer Trust** – Enabling an organisation to grow customer trust and participation through a dedicated and simplified customer portal and intentional investment to protect their information.
2. **Reduction of Risk** – Enable an organisation to be stay up to date with constantly changing legislative and compliance requirements from governments and other thought leaders to protect the rights of their citizens & countries across jurisdictions, i.e., GDPR.
3. **Unlock & Increase Data Agility** – Significantly increases organization's ability to change at a pace that meets customer's needs, respond to competitors or internal innovation by productising activities associated in building data products at scale.
4. **Security Companion** – Supplement and integrate with an organisation's arsenal of security products to protect their technology & customer information against internal or external unauthorised access.
5. **Increase Audit & Observable Intelligence** – Enable an organisation to collect & store tamper proof audit information for active and historic products & services to support non-repudiation claims and evidence for policy and customer consent.
6. **Faster value from mergers and acquisitions** – Standardise customer consent, privacy preferences, policies, and standards for newly acquired organizations.
7. **Customer Personalisation** – Enable the organisation to identify & respond to self-managed customer preferences and consent used to immediately respond to content personalisation and marketing opportunities.
8. **Transparency of information use –** Enable an organisation to provide centralised transparency to customers about the information held by and organisation, its relationship to various policies and products that uses the information for both active and historic products for all your channels.

Problem Statement

Consumers spend more time online than ever before, the time they spend online requires them to interact with consumer products and services that frequently requires personal information to uniquely identify the consumer or payment & address information to facilitate transactions and services.

Due to the global reach of the internet many products and services do not offer an in-person channel of interaction, meaning the consumer is faced with a choice prior to interacting with such a global organisation. While consumer may find it hard to resist marketing techniques, it is their responsibility to weigh value and risk to interact with an organisation that they deem trustworthy.

Beyond marketing techniques, products and services personalisation entice consumers by reducing friction, gradually building trust and rapport prior to collecting the information. Personalisation may come as the ability to add your spouse as a proxy to the service, it may offer support for a disability or nominate an emergency contact. Personalisation sets the expectation of customers that the product knows their context, i.e., likes and dislikes, and that information can be shared between products and services.

When a citizen interacts with public or state services, they no longer have the freedom associated with a competitive market and the choice of sharing information. They are compelled to share information to interact with public services digitally. Citizen's lack of choice can cause overly cautious behaviour resulting in low digital engagement preventing modernisation. Lack of transparency & control is increasingly fuel for misinformation campaigns. Public or state service, "digital citizenship" requires personalised content, transparency & control to stimulate engagement with the sector from where trust can be grown. As digital citizenship grows, many new challenges emerge.

The connected nature of the internet creates new challenges between critical personal & citizen information which can affect both public and private organizations alike. Customer information can be used to impersonate citizens interacting with public services providing different levels of application access into government systems and citizen information can be used to impersonate consumers to spread false political views or de-stabilizing fake news on social platforms.

Whether you are a public or private organisations, the ultimate challenge is keeping personal information safe.

Problem Background

Definitions

The following section provides a brief definition about 'Personal' and 'Person Identifiable' information.

Personal Information is defined as information about a person that is created and exchanged between an individual and an organisation as part of a transaction with a product or service.

Examples: A wish list of products, order history.

Person Identifiable information is defined as information that uniquely identifies the individual (natural or legal entity) performing the transaction.

Examples: Address details, date of birth, phone number, email address.

Introduction

Many organisations may be familiar with the problem statement; however, it is necessary to elaborate the problem, it's symptoms and root cause on a deeper level to empower organisations to identify it proactively and respond before it becomes an issue.

Understanding the problems, symptoms, and root cause behind the information-based products.

Personal information is exchanged between an individual and an organisation as part of a transaction or service. Over time an organisation changes the scope of services, requiring different pieces of to be exchanged to facilitate the transaction, in most cases the information is stored to speed up or enhance future transactions.

Services are delivered using technology which for the purpose of this document refers to the constituent parts of hardware and software. Organisations change their technology for several reasons such as improving customer services, reduce risk (internal or external to the organisation), benefit from technology improvements or maintain competitive advantage.

Organisational change may affect people, process and technology and therefor is considered complex. This complexity affects personal information in many ways.

Why is organisational change complex?

Change is complex as result of the ways we structure organisations to divide responsibility & labour, ensure management and wellbeing of workforce, better communication and organisational culture or geographic convenience or time zone compatibility to name a few.

Organisational structures are rigid and strive to get the optimal and stable working environment for the workforce. Unfortunately, an optimal environment for workforce that is also be beneficial to support product and services for customers at scale and pace while maintaining economic viability is a never-ending balancing act.

The nature of change in a competitive market or information legislation requires a level of responsiveness that cannot be achieved by restructures or aligning physical resources and therefor requires an evaluation into the way information products are built and how change directly impact them.

How does organisational change impact personal information?

The ways that critical personal information is impacted by organisational change:

The following will look how change dimensions of people, process and technology affects personal information.

1. Web application security protects personal information.

There are multiple security standards for the web and dozens of applications with different pros and cons that must be considered by an organisation to understand which standard is best for them and their customers. To adopt standards and increase security, organisations don't always have the luxury to build applications from scratch since they are already serving customers, any failure can directly impact revenue or existing services. Their applications may be at different levels of maturity or entirely different technologies where the systems were acquired as part of a merger or due to lack investment and maintenance. A security capability is complex and one of more teams operate across many fronts. There could be backend security for privilege access management, infrastructure, internal 'corporate' software, and client facing software or integration between internal applications or partner organisations for information exchange. While security changes are in progressed and coordinated on several fronts personal information remains vulnerable.

2. Customer judgement plays a critical role in the decision to share personal information.

Private organisations can use marketing strategies to exploit customer desire to divulge their personal information in exchange for the service. In the absence of customer desire, customers exercise their judgment prior to sharing information. Customer judgement is influenced by positive and negative experience, positive experience builds trust which takes time to develop such as through repeat transactions. Organisations must maintain customer trust throughout the change process, this may include preserving information between product versions, notifications to customers about technology changes and transparency around the use of historic information.

3. Technology change affects how data is collected, stored, and used.

Personal information collected as part of a service exchange will be stored in the technology of an organisation. As part of technology change the storage & collection technology could change, such as the website that the customer initially used to complete the transaction. Organisations must include privacy statements about the transfer of information as result of technology change in their terms of use for the information during the collection process. A technology change may invoke a jurisdictional change or change in geography with which the customer is no longer comfortable with. Any such changes must be communicated with the customer to ensure their consent is preserved.

4. Customer Preferences & Consent must withstand change.

Changing a customer product or service may require a change in preferences and consent. As result of change the customers' choice can become invalidated and containing preferences and consent for personal information no longer fitting the intent. Customer preferences and consent for their personal information is normally associated with the channel at which it was collected and supported by a 'terms of use' or 'privacy policy' and therefore must be changed on channel using a CMS (Content Management System) or another form of content syndication. Secondary use of personal information can be limited unless the original consent or customer preferences from the channel accompanies the personal information through the technology 'stack' as it moves to various systems for secondary use functionality. Consent granted in a new product has the potential to conflict with the same personal information in use by the original product. Unconsented use of personal information in new products and can significantly damage reputation.

5. What are the trade-offs between Product & channel independence?

Complex product and service dependencies often result in unintended service disruptions and impacted customers. To reduce dependencies software development breaks applications into functional layers to insulate each layer from change in subsequent layers, typically referred to as a stack. As the number of layers increases, information flow must be managed between the layers, a special layer for products or semantics is responsible to define what information belongs to a product. The trade-off, of the separation of layers results in lost information. Functional layers for audit, security & channel activity is unaware of the change because change was limited to the product layer, therefor historical audit activity may be inaccessible, alternatively to create a complete & transparent customer view it requires operational expertise for each respective layer to 'stitch' together the flow of information for the customer.

6. Soft Controls like Information Use Policy & Customer Consent is an important part of change.

Soft controls such as Policy is an important part of change that is updated to reflect a change in technology or business process for the information. The policy and any updates must be displayed to customers to acknowledge and, for large organisations with multiple products that could result in disclaimers of hundreds of pages that customers aren't willing to read or may find hard to understand. The lack of acknowledgement may prevent sales of products and services and increased friction will drive customers away. Legislative change timelines might force out of cycle updates to policy meaning that customers must re-read your policy often in its entirety. The policy content is generally current displayed as a catch all disclaimer on the 'channel' such as a website. The version at time of product or service exchange may require a special request or is entirely unavailable.

Conclusion

Change in an organisation highlights symptoms about its underlying complexity of systems, people and processes that can sometimes be built over decades. Change however, doesn't come by choice, even without the introduction of new products as seen in the public service sector, change might be forced unto an organisation based on global threats relating to customer data. In a globally connected world, change is unavoidable.

How does the DPF solve the problem?

The previous section described how organisational change can impact the stability of customer information and associated data products. Change is unavoidable if an organisation is to stay relevant and keep customer information safe and protected.

Change is an important part of keeping a Private Organisations relevant and competitive and in Public & State services change keep services up to date to best serve citizens of a country. If change is complex and unavoidable, what can be done to reduce complexity and avoid pitfalls.

The Data Product Factory (DPF) reduce complexity and simplifies change enabling you to create Information based products.

How can the DPF streamline and solve the problem posed by change?

The DPF uses several techniques to simplify change when building responsive information base:

1. **Headless** – The DPF is headless by design without a sequential workflow, steps, or internal dependencies. Each feature can operate independently providing immediate value within the feature. By doing so, time to value is enhanced and complexity is reduced as there are no complicated workflows, hand-offs with 'criteria'. Each feature has its own value as a complete product.
2. **Feedback** – The DPF is built with 'feedback' in mind, features are built expecting customers to enquire about to policy, subject matter experts can share knowledge, security endpoints provide feedback on handshakes and requests meaning information without the platform is readily available to those who need it.
3. **Self-Organising** – The DPF provides the mechanisms to group, categorise, and organise information-based products into groupings that is responsive the organisational, customer need including external contributors for research or academic projects.
4. **Self-Governing** – The DPF is built with governance in mind. This means it focus on providing agility through autonomy at feature level and enforce governance on the boundary using 'pull' approach enabling the relevant 'authority' to make the governance decision at the right time. Features including alignment with typical industry best practice for security, privacy, identity, and financial controls.
5. **Adaptive** – The DPF is built using techniques to reduce complexity over time making it easy to adopt and powerful to use. Each feature employs unique re-usable patterns rather than the DPF attempting to create a generic overall re-usable pattern. Techniques includes content syndication, voting, collaboration, crowd sourcing, reference data and re-usable configurations, templating etc.

Why does the DPF need a competitive edge?

The DPF was designed to protect customer information and build data products at scale however, it is not enough to have a good product if.

- its adoption is complex (workforce change & education)
- the running or implementation cost is very high.
- the return on investment depends on complex migrations & configuration that takes years to complete.
- it is seen as "redundant or duplicate" when compared to flagship investments still being implemented and waiting on return on investment.

For that reason, the DPF has made the following intentional design considerations to provide value early, adoption effortless and features intuitive.

What is the competitive edge of the DPF?

Industry dominating products are expensive, difficult to adopt, complex to populate with data. It takes multi-year change programs before you see the value with something that you can see the value in an afternoon.

1. **Software as a service (SaaS)** – Pilot it with a single person, a team, or a business unit, it's user-based licensing give you the flexibility to decide. The consumption-based pricing for traffic means once you have it up and running you only pay for what you use over the endpoints for any number of policies and products. There are no expensive implementation costs, meaning that you don't have to wait for the next funding cycle or a business case. It provides you with monthly and annual billing options and scalable options tailored to your expected customer base.
2. **Cloud Administration** – While the DPF is modern and new, it uses tried and tested roles & responsibility models rooted in sound financial practices providing separation of duties, notifications and governance between administration components meaning features are integration but not highly dependent. It includes pre-defined billing, security, administration roles meaning no configuration is required to meet common audit standards, whether you integrate it with your directory services or run it as a stand-alone solution. Using common standards, administrators will feel right at home meaning they can onboard users with confidence.
3. **Features Modules** – Enables individual teams to take their respective ownership over the respective area in the value chain of building data products. Teams can work in parallel creating policies and standards ahead of the product definitions, customers can register to the portal while products are being finalised and the product manager can finalise end point subscriptions. Collaborator feedback can be reviewed by data stewards without interfering with the complex backend processes of data provisioning. The respective ownership of feature models ensures there are always a contactable person who is an expert in their area that greatly assist in cross functional troubleshooting and knowledge sharing meaning experts spend their time doing what they do best rather than fighting a process dictated by technology or being blocked by artificial dependencies introduced by complicated management & governance solutions.
4. **Low Data Footprint** – The DPF is meta data driven that your business creates. It doesn't need to connect to back-end systems and it doesn't need to load large data sets to pre-populate schemas of databases. It relies on product meta data, that you create through an intuitive UI, bulk load, or copy & paste in a responsive web interface. The low footprint means it doubles up as an additional tool in your security arsenal increasing your security posture. The data in the system is yours, your organisation can export the information at any time to provide evidence in official records management or enterprise content management systems as evidence where your jurisdiction mandates it.

5. **Build for crowd** – Data Products can be complex, digital health, banking, insurance terminology can be a huge barrier preventing successful data product from being understood by customer or data consumers, understanding of specific domains or its nomenclature is referred to as knowledge. Knowledge must be sourced from experts inside but often outside your organisation. This software is built with the crowd in mind meaning peer review groups, medical informatics, policy research & development, or privacy or other minority groups can be invited to provide feedback on data products, policy and standards or glossary terms without having to acquire expensive licensing for them. Versioning, rating, and voting are just some of the functionalities used to increase knowledge for your organisation and customers alike.
6. **On the edge** – This refers to edge computing where data or processing is as close to the point where data is generated or in this case used as a data product or collected. It doesn't need deep integration or firewall changes into your network. It is a native cloud application and a true SaaS that sits outside your network acting as an authorisation service the can easily and securely determine when data product request should be terminated (on the edge) there and then due to access restriction, consent restricted etc. This means requests for data don't need to go into your network and use chargeable infrastructure or backend processing only to find out that it's not allowed to access the data because the customer have not given their consent. This means cost savings on erroneous data request round trips and an increased security posture. As all the requests are audited it provides a complete support for non-repudiation as a verifying party.
7. **Your software** - This software is jargon free; it doesn't introduce difficult industry terms that need workforce training prior to adoption. It uses intuitive web application-based interfaces and features use language familiar to each of the respective modules, policy uses authoring, draft, and publication concepts while security uses end points, API, marketplace, authorisation, authentication, and other familiar terms. The software is white labelled and designed for you to put your organisation's brand in front of your customers, not our brand. Maintain trust and confidence by using your URLs, all the subtle aspects that shows you value your customers.
8. **Build for the web** – This software is built natively for the web, it takes into consideration the complexities of web security standards, popular technologies and tried and proven concepts to provide security in the right places that by itself significantly uplift security posture of many organisations and integrate into current practices of Zero Trust, Client Identity (CIAM) to name two. It is also built for scale, while it is intentionally lite on data it, it didn't stop there, it is built for scale, resilience and operate with redundancy behind the scenes of an ever-growing base of operations it offers compatibility for many jurisdictions around the globe.
9. **Build for the future** - It is built for change leaning into the future with confidence and going beyond what is trendy like algorithms or language models. While keeping the future in mind, it is firmly grounded in solid foundations of data & information disciplines which are decades old meaning wherever you are in the maturity curve, it provides value to your organisation.
10. **Reduce complexity over time** – Typical software increases in complexity over time. This software is architected with patterns and re-useability tailored to individual features rather than a one size fits all approach. Data Products support versioning for quick AB Testing, Policies can be re-used as a whole or individual sections without having to re-write or duplicate it while it keeps full linkage to assess change impact of legislation across policy including individual data products and the customers affected by it.

About the DPF

What is the DPF?

The Data Product Factory is a white label Software as a service (SaaS) web application that integrates the domains of Information Security, Privacy & Data Use Policy, Customer Consent & Delegation, and Data Marketplace into a single Data Product Management Suite that operates on the "edge" helping you to go to market with fully compliant customer facing data products in record time.

Why is the DPF called 'Data Product Factory'?

The name for the Data Product Factory is critical to its success because it explains what the product does briefly, whether you are a user, executive or a strategic decision maker. The use of familiar terms in a new setting speaks to the common-sense approach and the vertical integration that provides its core strength while preserving the ability to inspect products, repeat and improve consistent processes meaning zero compromise in quality. It is a 'factory' that builds 'data-products'.

While the terms are familiar in a general sense, it is necessary to briefly explain the current state of the industry and call out some overloaded terms that are used in specialist industries.

What is a data product?

A data product is a 'complete' unit of data used to represent of concept necessary to solve a specific business problem and only that concept. It may represent a real-world concept like an 'invoice' or an address, it contains all the information therefor it is complete to perform a business service, such as a delivery. The courier only needs to know the address to deliver the parcel. In an advanced situation where a person must sign for the delivery, the data product might include an identifying attribute such as a signature.

The data product doesn't have extra or redundant data that is not immediately used to solve the business problem and is designed like a physical product that can be put in a shopping cart by using digital mechanism like an API.

From a non-functional viewpoint the data product provides consistency and sets the customer expectations to products in the real world. As with real world product, a product operates the same way every time or use it, this is important when the product must operate consistently across mobile and web channels. A product has instructions that specify intended use i.e., how to protect the user from harm' and avoid damage to the product. In data products, Policy and Standards perform a similar function, describing instructions about the data i.e., what you can do with it based on a specific rule concerning privacy and consent of the customer. A standard may be even set expectations, as with the "IP6 rating" you know a product can operate in a humid or wet environment.

Industry terms and their meaning in the DPF context

Several terms were considered and discounted for the DPF because the nature of the term could be misleading or underselling the value and strengths of the DPF.

The terms that resonated with the concept

Factory – The platform terms was changed to "factory" to speak to the repeatable, consistent & re-usable features as a "standard" to create product. It inherits dozens of well-known benefits of using a consistent or standards-based approach (especially for empirical measurement. The term factory has stuck.

Product - The word product as in physical product means complete, ready for market, quality assured and compliant, as a successful product should be (heavily inspired by BMW factory \ Devops, lean enterprise and the works of Gene Kim). The term data product is well understood but as of the latest research in Gartner there are no bespoke platforms \ software suites dedicated to the build of data products. This name Data Product was combined with Factory to form, the Data Product Factory.

Discounted terms and rationale

Data Readiness Platform - Readiness is an existing data warehousing (DW) term, however, prefixing readiness with "product" isn't in high use and the DPF goes beyond making the data ready.

Data Orchestration Platform - Orchestration is an existing term; however, it doesn't deal with aspects such as legal \ security \ privacy and is typically narrow in scope. It is associated with combining data from different Api's i.e., API orchestration, it also implies a certain level of automation. The DPF has is not an automation platform and it deals with a much larger scope and orchestration.

Data Compliance Platform - Compliance "Platform" is very accurate however, the existing use is very risk focused, the scope typically doesn't include security or consent or data catalogue management. There are flagship compliance platforms in the Gartner Quadrant and the DPF provides many other functions beyond risk & compliance. The DPF offers crows source, content syndication, data schema and meta data management as well as privacy settings customizable by users.

Data Platform – A Platform is typically something to build on, it might suggest data is stored in the platform (which is not the case, only metadata is). In that this product could be considered as a gateway, portal, i.e., off to the side authorization & policy service (which has limitations in scope since API auth doesn't deal with data, and policy doesn't deal with privacy in this context. The DPF doesn't store copies of data from your repositories, your organisational data remains in place and therefor the DPF isn't a platform.

Data as a service platform - Data as a service - limited in scope that DaaS isn't complete, it doesn't come with auth (consumer) and typically doesn't come with policy integration. The DPF provides many features beyond making data available as a service. It enhances your data with meta data, crowd or expert sourced glossaries and policies.

The DPF Ecosystem

The DPF ecosystem is the collective description of features that make up the DPF. The DPF features are value stream oriented and is designed around cross cutting barriers with everything needed to build data products at scale, i.e., Customer Consent, Policy, Data Assets, Business Glossary, Security, Authentication & Authorization, Compliance & Audit.

The table below provides a comparison between the typical industry vertical, the DPF feature and the business value.

Feature	Business Value
Privacy Center	Customer 360, Customer Accounts, Customer Privacy Settings & Preferences Customer Consent Customer Delegates
Data Product Manager	Data Product Catalogue Custom Meta Data
Community Center	Business Glossary
Policy Center	Policy Authoring Policy Syndication Audit & Compliance
Subscription manager	Secure Data Access
End point manager	Protected Data Use Audit & Compliance

DPF Features

1. **Privacy Center** - Where your customer specifies their privacy preferences, grant consent or invite delegates and view data product audit on the data you have about them.
2. **Data Product Manager –** Where your business defines the products they have and the data attributes (schema) that makes up the product and meta data such as policies and purpose of use associated with the data product, and data asset groupings(meta data).
3. **Community Center** - Where knowledge is crowdsourced to provide meta data such as glossary, terms, corrections, or validations by internal and external specialists alike.
4. **Policy Center** - Where your business specifies policy and standards which can then be associated with data products.
5. **Subscription manager** – Where you're a business specify subscriber, pre-share keys and trust tokens to query the endpoints for during authorization requests.
6. **End point manager** – Where your business manages end point configuration and monitor insights \ usage.

Business Outcomes

1. **Customer 360** - See all the data you have about a customer in one place.
2. **Customer Accounts** - See all the customer's business identities \ business contexts in one place.
3. **Customer Privacy Settings & Preferences** - Enable your customer to manage their privacy settings in preference for the data you have about them in one place.
4. **Customer Consent** - Capture consent from your customer for the data you have about them for all channels.
5. **Customer Delegates** - Enable your customers to nominate trusted persons as delegates.
6. **Data Product Catalogue** - Manage your Customer Data Catalogue in one place.
7. **Custom Meta Data -** Add custom meta- or reference data to increase the quality of your data catalogue holdings.
8. **Policy Authoring** - Create Re-usable Policy & Standards that can be associated with data catalogue items to improve quality with standards and protect access with policy.

9. **Business Glossary** - Add and associate business terms and their descriptions, synonyms and example uses to a data product.
10. **Audit & Compliance** - Rich audit & evidence for compliance by associating policies and standards to your information holdings.
11. **Secure Data Access** - Enable subscription-based access to data holdings.
12. **Protected Data Use** - All subscription-based requests are processed by the Policy service to protect data against unrestricted use and provide full evidence of usage & requests made by subscribers.

Ecosystem Value

The DPF allows you to realise business value from data that is otherwise very complex to achieve. By integrating features within the DPF there are secondary benefits realised when operational activity from one feature area can enrich the use of another feature.

The sum of value is greater than individual features.

In a typical organisation these features are operated from silos between product channels, logging and monitoring, back-end services, and API load balancing to name a few. Connecting the activity of operational data is a complex operational undertaking even before turning it into valuable insight.

Analytical & Usage Insights

In the DPF the operational activity resides on the same platform enabling you to draw product insights like never before.

Refine & Optimise Policy – Is your information use policy too generic or too specific, can your policy statements be re-used between products and jurisdictions. Is your policy protecting the data & use?

Data Asset Structure - Is my data assets structured appropriately for use in my organisations' products and services or can the cardinality between a data asset and API endpoint \ request be improved to reduce round trips?

Product Innovation - What are the contexts that the data is being used for i.e., purpose (research, other products, composition etc.). Do I have Api's requestion additional uses? i.e., Digital International Patient Summary (IPS) vs. Problems.

Channel Limits & Optimisation – Which APIs are called more frequently and other API analytics, performance, volume, audit, security. Is my organisation building the right API's?

Fraud & Duplication – When do I differentiate between my customer account and their identity. Which products should use which identity and do I have consent to match entities. Customer resolution (entity resolution) across contexts by binding to data assets context rather than systems.

Product Vs. Channel - Can I improvement my consent & terms of use to unlock up potential uses of data in secondary products and channels?

Standardise Usage Reporting - Data egress is standardized and controlled via Subscription and Endpoint manager collecting audit, usage, and monitoring for individual data products regardless of channel.

Complete Transparency - Data access \ usage and sharing always adheres to client consent. A data request can provide a full & transparent view about any denial of data access whether it was as result of lack of consent, incorrect scope request from API or an out of data policy statement, all retrievable via RESTful API

Non-repudiation - All endpoint requests & data access policy requests, policy & use activity are fully audited and able to withstand any repudiation claims across the transaction chain.

Conclusion

Beyond the functional value of compliance, security, and customer confidence the DPF offers extended value in one place that would additionally require additional procurement of stand-alone products.

Why is there an opportunity for the DPF?

The typical estate reflects a capability & technology centric architecture with many handoffs, dependencies and components that must work in concert to unlock data for consumption, protecting it, applying privacy and consent that may vary depending on channel and customer context, while having to evidence it's use and change in policy over time.

The Typical Enterprise Data Estate

The Enterprise Data Estate is a collective term for all the people, process and technologies use by the business to build products and services for their customers.

To effectively use data an enterprise must establish, manage, and coordinate dozens of capabilities from legal, security, privacy, data ingestion and consumption. This uplift of data transformation programs can take decades to setup and even longer to implement due to their complexity and ever-changing landscape.

How does the DPF solve this problem?

The DPF does what Lean, Scaled Agile(SAFE), Devops, product & value-based thinking did for the software industry by making data products agile to bring value to customers faster for complete and compliant data products.

The Data Product Factory introduction

This *value chain-oriented* product factory has all the functions required to build complete, compliant & consumption ready data products.

It is complete from point of capture to consumption, the data product factory features ensure compliant, secure, and consented data products with full audit transparency that builds measurable customer trust and increase participation using analytics built on activity in the same factory.

By using this product data is consumption ready faster, it means a faster time to market for data products, centralised compliance, transparency, audit, and data product management which unlocks sales & marketing features for individual data products such as product uptake, client engagement & sentiment, policy's fit for purpose.

The product factory connects your internal experts in the fields of security, privacy, legal and customer consent in streamlined features modules for vertical integration with zero compromise on quality.

The factory follows a loosely coupled architecture and act as-a-service enabled layer of meta data between your physical data repositories and data product endpoints. This offers compatibility with virtually any data repository to, supplement in-house capabilities and protects data products with governance at the edge, secondary benefits are that it avoids data duplication, unwanted caching, jurisdiction, and sovereignty concerns.

Does it work for any business on the maturity curve?

The following two use cases show how the Data Product Factory can deal with age old “issues” or new and currently trending issues. This evidence highlights how value can be derived regardless of where your business is on the maturity curve.

Use case for currently trending themes “AI, Ethics & Language Models”.

When a data product is created on the data product factory it links to a Policy specifically designed for AI, Ethics and Automated Decision Making. As soon as the Policy is published it is linked to a data product. With immediate effect, existing customers receives a notification on the policy update prompting them to accept the policy. Their preferences are saved in the privacy centre and any service endpoints in place remain as is, however, if their purpose for using the content is not consented. Their claim to the data is denied.

Use case for traditional issues.

When multiple data products contain the contact details of a customer, the data product manager can use the product factory to add custom meta data attributes to the product used to flag preference and priorities between them, rather than somewhat abstractly calling either master data. An example of this would be an attribute that flags a specific contact detail as the preference for email or preference for physical deliveries. Customers will receive a notification about the update on the data product and specific their preferential contact details across one or more products. Existing endpoints can be modified to process the additional information, left as is as receive a message stating the contact detail usage or a REST based implementation (self-describing) maybe provide programmatic access to the preferential contact details.

What other scenarios would benefit from the DPF?

For any number of reasons an organisation might think that this problem of building data products at pace and scale is something for only sophisticated organisations, then think again. The DPF’s uses come in a number of different scenarios , some of the scenarios operate at organisational level and an organisation might be mature enough to identify the problem and symptoms however, some advantages of the DPF requires a deeper understanding of operational process, and the challenges of technology& operational teams have become so ingrained in a business process that it seems natural, since it’s always been done that way.

Potential use cases for your organisation:

The below characteristics signal a high probability that your organisation could significantly benefit from the adoption of the DPF in support of your operational processes.

An organisation that has the following characteristics and needs one or more of the following:

Multiple Data Repositories - An organisation that has multiple data repositories.

1. a central view of all your data assets without being bogged down in specific implementation or technologies of each respective repository.
2. Discover and view their information assets they hold.
3. Identify products and services and dependencies between information assets.
4. a 360-degree customer view across multiple repositories.

Multi-Channel strategy - An organisation that has multiple channels for engaging with your customers.

1. A consistent security pattern across channels to authenticate your customers.
2. Gather insights from customer product interaction.
3. The channels rely on policy & privacy statements embedded in your channel footers.
4. The need to compare product performance to a previous version or a different channel.
5. Consistency between privacy settings & controls between channels.

Security & Compliance - An organisation that operates in a regulated area and need to evidence your level of compliance to set piece of legislation.

1. The need to ensure your data use policy is up to date with your latest data product innovation.
2. Compliance with GDPR, Privacy Act and similar types of legislation.
3. The need to provide audit about applications data use & purpose.
4. Endpoints must have periodic reviews to ensure they are compliance.
5. There is a need to provide customers with evidence of the information you have about them!
6. The need to manage privacy.
7. An organisation with a need to product customer information.

Information Sharing – An organisation that shares customers information.

1. The need to share information with another organisation.
2. Definitions about information being shared and what they are allowed to do with it.
3. The use of policy & standards for information sharing
4. The need to formalize information sharing terms using MOUs (memorandums of understanding) information sharing agreements, contracts.
5. The need to share data of their customers (including the privacy settings associated with the data, i.e., purpose of collection)
6. The need to expose customer data via open API's that must adhere to consent and purpose of use.

Customer & Consent based products – An organisation that deals with customer information and a breach of data undermine customer trust or customers.

1. Customers' need to know what data you have about them and what you do with it.
2. An organisation that has products that requires consent to access and use data.
3. Customers' need to self-manage their privacy settings for the data they have about them.
4. Customers' need to delegate to another individual, i.e., rates payer (both partners) accesses the same account. Council property management might be delegated to facilities maintenance.
5. The need to simplify consent management that span multiple datasets by using policies.
6. There is a need to communicate and request additional consent for customer information to expand to purpose of use beyond the initial collection of the data.
7. Want to unlock potential of data by creating transparency about how it used to improve services.

Customer Context - An organisation that differentiates between its customers & their service contexts.

1. The need to identify different customer context for an individual i.e., a mobile contract owner VS a broadband or electricity subscriber.
2. Enable customer to manage and update their information to keep it current.
3. The need to match a single natural identity with multiple business identities.

Complex Information – An organisation that relies on subject matter experts to define glossary & policy through external collaboration, reviews, and versioning.

1. The need to embedded information product glossary with the product
2. The need to cater for complex visual standards like medicine labelling.
3. Data product standards must be accessible by everyone and customizable by channel to ensure consistent products.

Appendices

The following appendices provides additional details about the industry position of the DPF. The DPF includes a roadmap useful to understand on-going development of the solution. The appendices extend and elaborates on the challenges associated with changes in an Enterprise Deep Dive.

How does the DPF integrate verticals?

This software, a data value stream platform is modelled on the data value chain, cross cutting everything needed to build data products at scale, i.e., Customer Consent, Policy, Data Asset, Business Glossary, Security, Authentication & Authorization, Compliance & Audit.

Roadmap

Beyond the initial development of the DPF it includes a roadmap for the on-going enhancement of the product ecosystem. The roadmap can give investors confidence about the on-going viability and value that the DPF can create beyond the startup phase.

1. **Policy Authoring v2** - Like, vote, co-author, policy sections to fast track policy & standards authoring.
2. **Collaborate** - Built in collaboration with subject matter experts, reviewers or external assessors in the same ecosystem where the data schema, glossary and policy exists**. (Requires: Policy Authoring v2)**
3. **Information Asset Management v1** - Group datasets in Business Information Asset Groups to identify opportunities of growth & investment.
4. **Information Asset Management v2** - Lifecycle management, associate assets with investment & life cycle management. **(Requires IAM v1)**
5. **Digital Asset Management v1** - Associate digital assets to information asset counterparts to understanding intricate relationships between your technology & your data **(Requires IAM v1)**
6. **Information Asset Management v3** - Capture investment & Associate Initiatives with assets **(Requires DAM v1)**
7. **Smart Contracts -** Digital contracts suited for the exchange & enrichment of information **(requires Digital Asset management)**

Platform \ Industry Vertical	**Vision & Scope**	**Features v1**	**Roadmap**
Consent Management \ Platform	Provide centralized customer consent, privacy settings & preferences, include delegation in context of individual asset	1. Customer Privacy Setting & Preferences 2. Customer Consent 3. Customer Delegation	
Policy Writing \ Risk Management Software	Policy authoring, versioning directly in context of the data asset. Policy that comes with teeth, the policy is backed by a policy engine that evaluates data requests against the policy, which is a sum of customer preferences, internal policies, and API subscriptions.	1. Policy Authoring 2. Compliance	1. Policy Authoring v2. 2. External Collaboration
Open Data \ Data Hub	query policy, to discover open data assets or consented access to data assets	1. Policy Service	
Master Data Management	define & re-define and iterate master data assets as the unit of measure instrumental to convey business concepts, to which you can apply policy, consent with high re-use but without physical coupling to technology, database integrations and locks-ins to maintain providing flexibility to experiment	1. Customer Data Asset Catalogue 2. Feature Rich Catalogue	1. Information Asset Management 2. Digital Asset Management

	with different data products while operating within compliance and consent		
Customer Identity & Access Management (CIAM)	Bind external BYOIDP or mandated identities with your customers' business identity to get a single customer view while retaining individual contexts by channel or product	1. Customer Accounts 2. Customer 360	
Data Catalogue	generate data assets with attributes and meta data and add classifications using properties to associate, policy with simple labels that can be re-used across assets enabling reporting across labels	1. Customer Data Asset Catalogue 2. Feature Rich Catalogue	1. Information Asset Management 2. Digital Asset Management
Data Platform	Store meta data only and a highly secure environment de-coupling the front end from back end reducing security risk significantly, avoiding lateral or supply chain type attacks	1. Data remains at source. Only policy, consent settings, catalogue items, meta data, glossary, and audit information exists natively in the product.	
Business Glossary \ Data Dictionary	provide a high context glossary directly coupled and use by policy, data assets, the customer and enable crowd sourcing of expert knowledge ensuring the business, technology and customers share a common understanding of the data held by the organisation and what it is used for	1. Business Glossary	1. Policy Authoring v2. 2. External Collaboration
API Authentication \ Authorization API Market Place	Enable API requests to identify the requests, directly against the policy service that can translate requests against the define data assets, and ensure compliance with policy, customer consent or delegation while being fully auditable for non-repudiation and set rate limits for individual data assets, and collecting performance and audit information for all request activities	1. API Subscription Management 2. Audit & Compliance (Security) 3. Nonrepudiation 4. Protected Data Use 5. Secure Data Access	1. Smart Contracts
Customer Data Platform	Build an abstraction layer between internal systems and business needs to create loose coupling meaning you can have different views of a customer and apply different policies to each	1. Customer Accounts 2. Customer 360	

Market Comparison

The market is abounded with data products and tools. The next section will provide insight and key differentiators between existing tools and the proposed DPF.

The table shows verticals in the industry. Each vertical has respective leaders, i.e., IBM Informatica - for MDM. Currently, for an organization to build a successful data product they will need several platforms. The platforms tend to stay in their vertical often for decades. The adoption, cost, and complex implementation. Customer value is not realised until the last part of the value chain is in place, only to find out that their competitor has deliver their product to market months ago.

In comparison, with the DPF an organisation can deliver superior quality data products giving their customers trust, confidence & and on-going evidence through their participation in policy, privacy and consent for data use enabling while keep the ability to quickly iterate and fast follow with new and improved products.

How do organisations approach data?

An organisation doesn't typically intent to build cumbersome IT systems. They don't intend on leaking customer information, and they don't adopt weak security or contradicting policies.

If organisations set out with the best intentions, why is it that they end up with technical debt, poor security postures and inflexible architectures? Data complexity is ever increasing in scale and the allure of identity and theft of personal information means that organisations must product themselves at a scale and pace like never before.

The follow section will take a deep dive in the typical organisation that has been operating strong for over a decade and after merging with a new organisation find the need to develop data products faster.

Enterprise Data Estate – Deep Dive

Behind the beautiful facades of stylised rounded corners our customer portals' rich interaction is reliant on customer data. Customer data that resides behind protective mechanisms of a business, the protective mechanisms fall in the domain of cyber security and can be physical or digital such as network, firewalls, data-services, and gateways.

Customer data may reside in many individual systems, networks or in one or more data centres "clouds" and up to potentially one, cloud for each respective service or engagement the customer has with the business. In the case where a company buys a flagship product from a large multinational corporation, data could often reside entirely confined to the boundaries of that application. These systems are typically thought of as the back end.

As example, your voice call logs will be in the contact centre system, your email correspondence on an email server, your personal details in a customer relationship management system otherwise known as a CRM and your banking details in a Financial Information Management System or FMIS. As the products and channels of a business increase, the likeliness of your data being in multiple systems increases as well, each one of these systems must be protected.

To simplify access to the data by other systems and downstream consumers, businesses often rely on centralisation by having connectors from various systems of record that integrates with a central point, this is generally called data integration for point-to-point connections or ELT, ETL (Extract, Transform, Load) for batch, streaming which includes making a connection between both the source and target of the data and some manipulation of the data either before or after loading. Historically we associate centralisation with a data warehouse but in modern times it could be known by many names like, data lake, lake house, streaming analytics, data platforms or cloud data warehouse, big data, or blob storage.

Centralisation of data for internal consumers increases security because access is centrally managed, and centralisation typically occurs in networks with layers of security. While mature organisations have moved to a "trust no one" model when it comes to granting access to this central repository, many organisations still trust connections to this central repository when it comes from the same business network or a trusted software, i.e., report visualization software or a direct query from a service. Security access controls are typically assigned to intermediate trusted software, services or connections which are in turn managed by a different set of individuals with specific expertise in that software, service, or connection.

Centralisation typically follows a hub and spoke model where individual systems of record are spokes connecting to a central data hub. While fast networks, growing cloud interconnectivity and clever caching mechanisms are enabling logical centralisation only pulling data to the hub as and when needed, generally data is physically copied to the central point, i.e., a copy of the data is made including historic records for analysis over time since systems of record are streamlined to keep just the latest record or may have cost or storage implication when retrieving archived data from tiered storage. Historical data over time is how reports like power usage or mobile data usage over a period of several months are produced.

The drawback of centralisation is that you can't always make an exact copy of the data, the email server stores internal data not available to other systems like audit records or highly technical data, the contact centre technology could be proprietary, or the large data types such a video (bus lane infringements or body cam footage) and images (think x-rays) may be too expensive to transfer or duplicate, the FMIS data is financially sensitive so financial audit controls might prevent centralisation.

The result is that some data is centralised and some not, it is also difficult to tell where the data came from (referred to as lineage), since both the contact centre and the email server has your first name with respectively slightly different spelling and the financial system refers to a legal name which could be entirely different. The process of picking the correct version to get a single view is called normalisation which is a specific data warehouse term to remove redundant copies of the data as defined by business rules, more advanced processes using machine learning can use statistical probability to determine the full and correct name and even recommend possible nickname using a process called entity resolution. The ability to recall what changes were made to the source data considering business rules are referred to as traceability.

Centralisation may further combine data from source systems into a *complete customer view, where customer data is represented as a single place to query for all data in single data repository. At this point, the origin of the data, your login and associated audit information, consent granted for usage for a specific purpose of the data is only detected as remnants given that including such information may not be available in the connectors or the information would increase the cost, latency, and complexity significantly *ironically an incomplete view of the customer.

Now that the various copies of your data are centralised, it is easy to connect to and use. especially for purposes different to what it was collected for in the first place, given the weak evidence of original consent and purpose. Any applications that want to connect to this information can now do so, through trusted tools that doesn't differentiate between purpose of collection vs use. The solution for this is to add governance tools that is expensive, and businesses must be of sufficient scale to dedicate the resources to successfully implement and operate it on an on-going basis.

When you update the information in the central system it often cannot determine which address should be updated, i.e., the contact centre, email server, CMS or FMIS. While there are patterns such as Command Query Responsibility Segregation (QCRS) to manage this it adds significant complexity to the central repository that resulting in two types of centralisations i.e., an analytical data warehouse and an operational data warehouse (supports write-back to source). Businesses of sufficient scale can invest in master data management tools and define the business rules that determines the system that holds the authority over a specific piece of data to ensure that the CMS holds the master and FMIS hold a copy, which as immediately apparent, isn't without its issues, resulting in additional data to be created as example Billing Address Vs. Shipping Address.

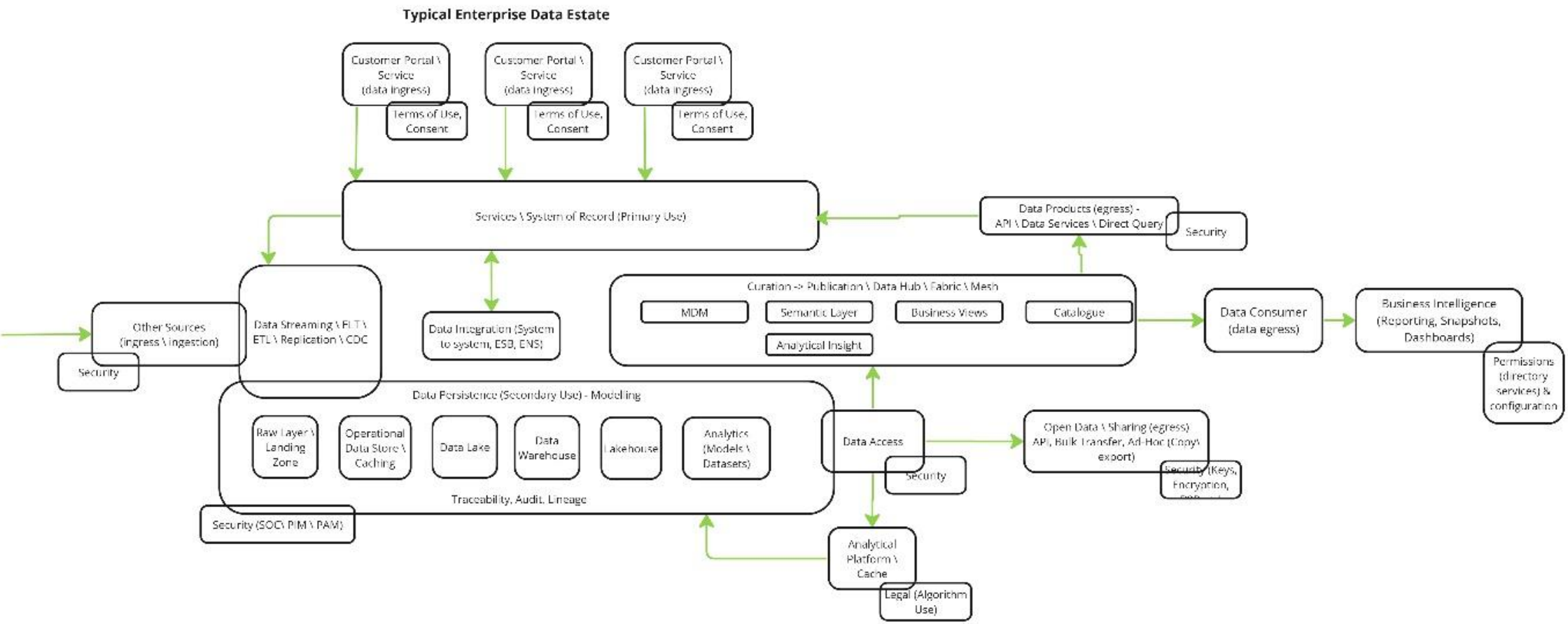
The business landscape isn't static and while governance, master data management and selective centralisation all play a role in reducing complexity the systems of record change over time. New functionality, upgrades or replacements may affect data integration, ETL, ELT, Network trust, Software configuration and centralisation. Data can quickly become out of date and change synchronisation can be complex which results in poor overall data quality. You want to revert to an older application that uses the email server's address but since it's been upgraded to a new version, the centralised data schema is somewhat different, and you might have to support two products until you can notify all your customers about the update before you can switch to the new application.

In the systems of record there are system documentation or supporting systems that guide staff with knowledge how to use the system i.e., contact centre and explain what certain terms mean, time in queue, after call work duration, everything you need to know about complexities of the data attributes within the system of record. Contact centre staff might even capture their own insights or specific terms to regions or cultures and learning from their customer engagement. For various reasons other than technology limitations or low perceived value, this knowledge seldomly forms part of the centralisation of data.

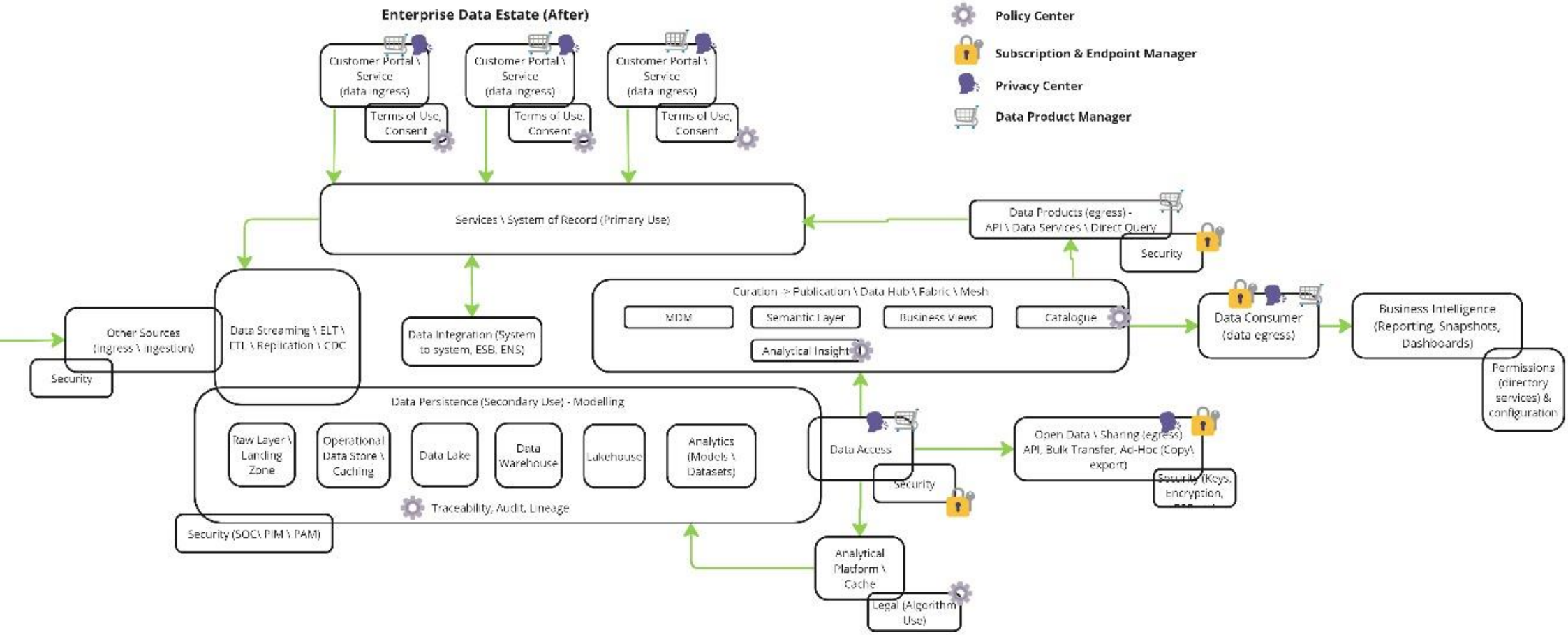
To address this missing knowledge problem businesses of sufficient maturity and scale has dedicated resources to manually capture the knowledge. The knowledge can be captured to varying degrees of detail but is typically known as meta data, data about the data. The meta data is captured in a meta data- or data catalogue systems, or business terms in a business glossary. This ensures that anyone with access to the central copy of the data may be able to understand some of the operational terms & context from the system of record. This information is slow changing, but requires dedicated resource typically called data stewards or custodians to ensure data is up to date and the business context is accurate.

Customer portals typically requires an account for sign-up, and it is best practice not to share your account information however, services are often shared. Billing for property rates & taxes are shared by the owners, parents or guardians may share custody to a dependents health record information. Depending on the service and sensitivity of information, it is access to a spouse or partner, or other identity requires additional verification or proof, sometimes the evidence is unobtainable, (think of a non-citizen but visa holding grandparent caring for a grandchild while their parents are overseas. The parents can consent to the grandparent acting as a guardian in an emergency, but the system may reject this claim based on a lack of evidence. The wishes of the customer to grant consent is often undermined due a lack of system functionality. Businesses must modify all channels to support delegation and standardise roles (what the delegate can do) & relationships (what their relationship is to the delegate) or use manual processes to provide verbal or written approval which may be added as a note to the system or to create profiles for each delegate as used in banking operated by a clerk rather than self-service by the customer. Notes are often not centralised due to variability of size which impacts predictability of data transfer a central repository.

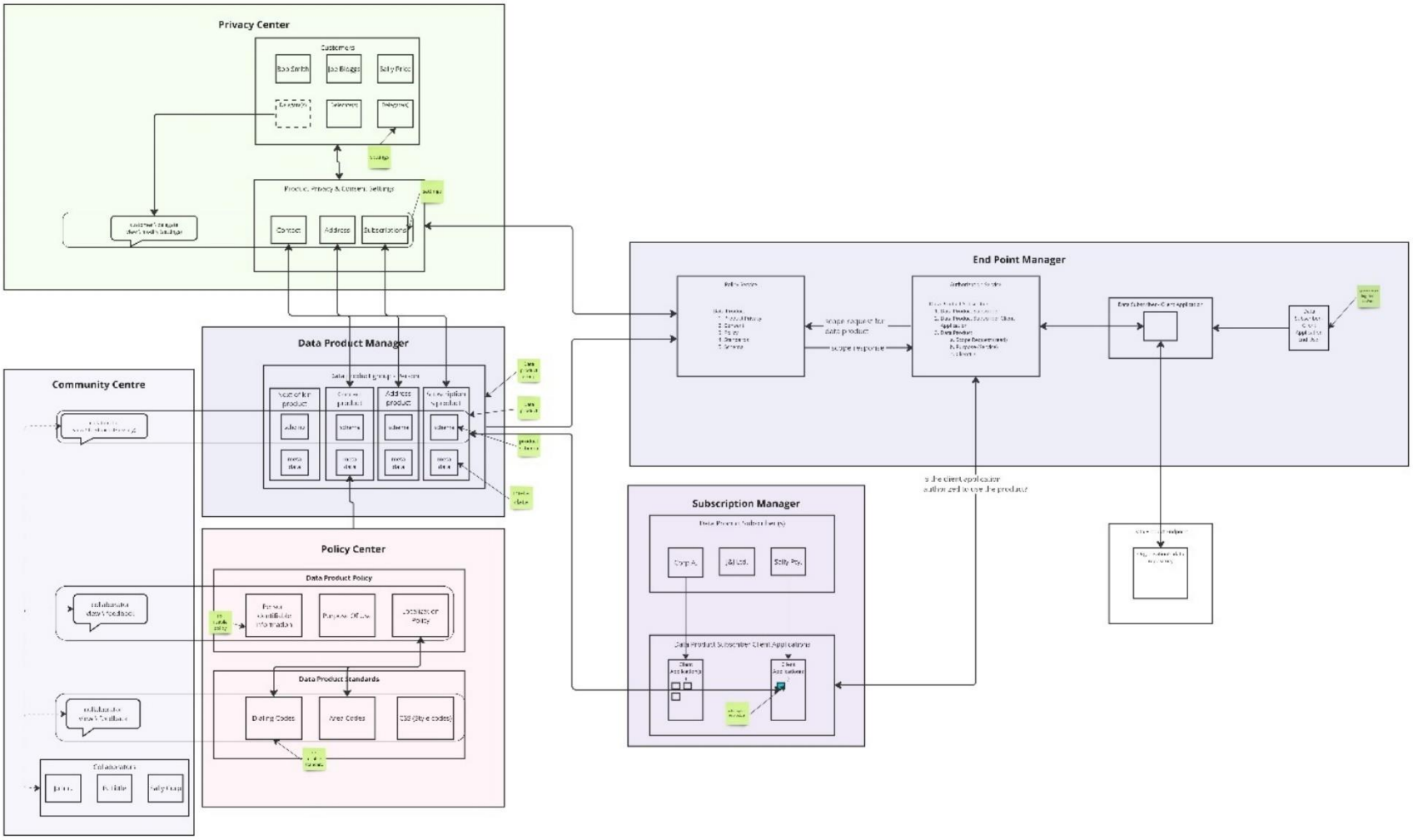
Enterprise Data Estate (Without the Data Product Factory)



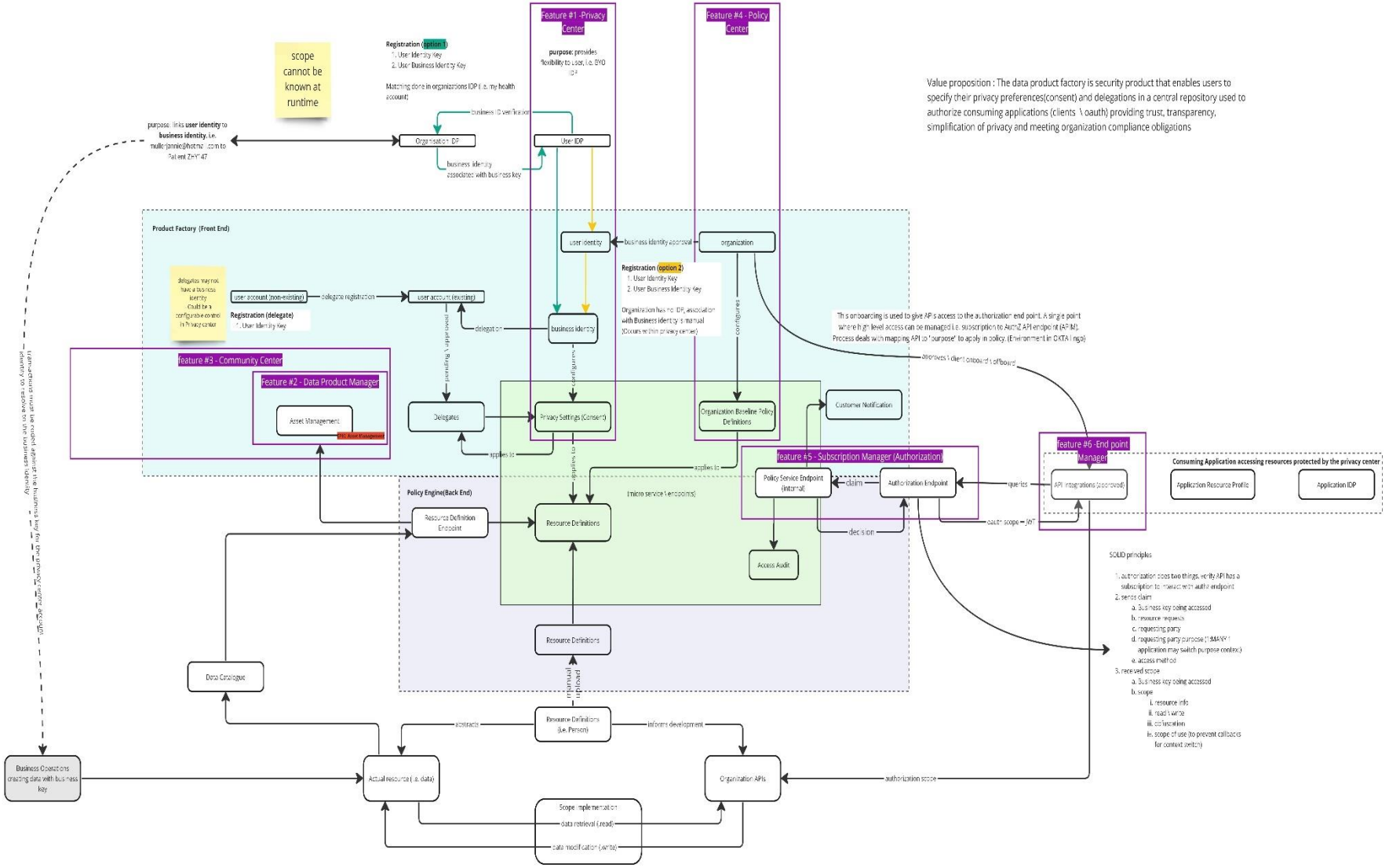
Enterprise Data Estate (With the Data Product Factory)



Conceptual Architecture



Logical Architecture



Roles & Permissions

Roles Hierarchy

1. Business user - System Admin
    1. business user – Security admin
        i. business user - data product owner
            1. data consumer - data product subscriber (subscription owner)
                a. data consumer - client application
                    i. data consumer - client application end user
        ii. business user - subscription owner
        iii. business user - system designer
        iv. business user - customer account administrator
            1. End User – Customer
                a. End User - Delegate
        v. business user - content writer
            1. End User – Collaborator

Roles & Responsibilities

Role	Responsibilities
Business user - System Admin	Business User: System Admin (Type of person) The person that deals with roles for the platform 1. As a system admin I want to sign up to the product 2. As a system admin I want to configure backup credentials, MFA and store a code in case I lose my credentials (Break glass account) 3. As a system admin I want to nominate a backup user that can act in peer in case I forget my details (break glass account) 4. As a system admin I want to integrate with my directory services for SSO 5. As a system admin I want to link my tenancy to my custom domain
business user – Security admin	Business User: Security Admin (Type of person) The person that manages role assignment 1. As a security admin I want to assign business users to system roles 2. As a security admin I want to add \ remove \ manage data subscribers 3. As a security admin I want to add \ remove \ manage data subscriber client applications 4. As a security admin I want to see all role changes audited
business user - data product owner	Business User - Data Product Owner (type of person) A person working on the data products including ownership aspects, management, stewardship, and curation to capture the information about the data product. 1. As a data product owner, I want to add \ remove \ manage product groups. 2. As a data product owner, I want to add \ remove \ manage data product 3. As a data product owner, I want to add \ remove \ manage data product attributes to define the product schema

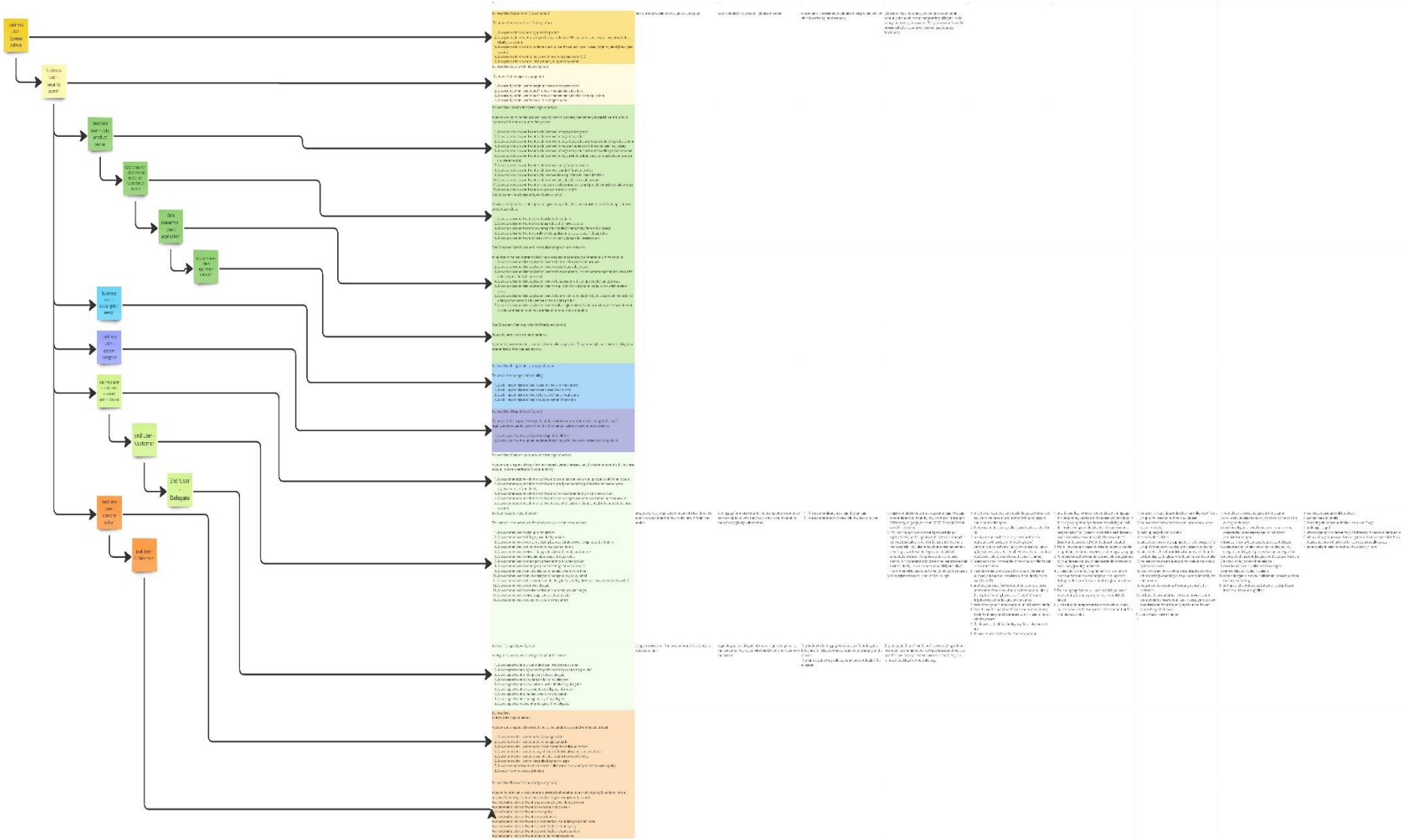
	4. As a data product owner, I want to add \ remove \ manage attributes descriptions to be used in a glossary 5. As a data product owner, I want to add \ remove \ manage data product attributes to define product meta data 6. As a data product owner, I want to add \ remove \ manage a list of attribute values to re-use between products (i.e. reference data) 7. As a data product owner, I want to add \ remove a policy for a data product 8. As a data product owner, I want to add \ remove a standard for a data product 9. As a data product owner, I want to add \ remove client applications for data subscribers 10. As a data product owner, I want to add \ remove data subscribers to a data product 11. As a data product owner, I want to invite external collaborators to view and provide feedback on a data product 12. As a data product owner, I want to run product reports & insights
data consumer - data product subscriber (subscription owner)	Data Consumer - Data Subscriber (type of business entity) A business entity that has a subscription to a given data product, it is a pre-requisite to enrol client applications to access data products. 1. As a data subscriber I want to be onboarded to the platform 2. As a data subscriber I want to view data products that I have access to 3. As a data subscriber I want to view data product details (Schema, Policy, Standards, Glossary) 4. As a data subscriber I want to enrol my client application to access a specific data product 5. As a data subscriber I want to have a contract to specify data product access details
data consumer - client application	Data Consumer - Data Subscriber Client Application (type of code \ software) An application that can programmatically make a request for data through an integration with the endpoint. 1. As a data subscriber client application, I want to be enrolled to access data products. 2. As a data subscriber client application, I want to query data product details 3. As a data subscriber client application, I want to have a contract to I can set customer expectations (rate & other limits, response times, failure codes) 4. As a data subscriber client application, I want to be associated with a unique code for audit purposes. 5. As a data subscriber client application, I want to Application has subscription key i.e., access which provides access 6. As a data subscriber client application, I want to be enrolled into the platform by the security admin for a data product owner to add \ remove access to a data product 7. As a data subscriber client application, I want to call a single service with data product request information that provide authorisations for all the authorisation for data product endpoints
data consumer - client application end user	Data Consumer - Client Application End User (type of person)

	Requesting party in terms of oauth parlance. A person that accesses the data via a data subscriber client application. The person maybe be a customer, delegate, or other entirely different requesting party.
business user - subscription owner	Business User: Billing Administrator (type of person) The person that manages platform billing 1. As a billing administrator I want to see the invoice for the platform 2. As a billing administrator I want to see a breakdown in costs 3. As a billing administrator I want to be receive financial notifications 4. As a billing administrator I want to update payment information
business user - system designer	Business User: Designer (type of person) The person that is responsible to style the platform with the communications & branding for the specific organisation to ensure it aligns with their brand to maintain customer trust and brand presence. 1. As a designer I want to configure the design of the platform 2. As a designer I want to upload header and footer images for the external presence of the platform
business user - customer account administrator	Business User: Customer Account Administrator(type of person) A person who is responsible to perform business activities such as associating the customer account with a business account, i.e., identity verification & account binding. 1. As a customer account administrator, I want to be notified when a new sign up occurs to bind to an account. 2. As a customer account administrator, I want to specify the mandatory profile attributes needed by the organisation to verify an identity. 3. As a customer account administrator, I want to bind a customer identity to a business account. 4. As a customer account administrator, I want to bind a delegate account to a customers' business account. 5. As a customer account administrator, I want to see which customer identities needs to be bound to business accounts.
End User – Customer	End User - Customer (type of person) The customer is the person who the data is about, a.k.a client, resource owner. 1. As a customer I want to sign up to the platform 2. As a customer I want to bring my own identity provider 3. As a customer I want to re-use my existing business identity provider to sign up to the platform 4. As a customer I want to bind my identity to a business identity 5. As a customer I want to view all data product(s) that the entity has about me 6. As a customer I want to view data about a specific data product 7. As a customer I want to manage my privacy settings for a data product 8. As a customer I want to manage my consent settings for a data product 9. As a customer I want to invite a delegate to manage consent on my behalf

	10. As a customer I want to invite a delegate to manage privacy on my behalf 11. As a customer I want to be view the state of a delegate (i.e., pending, declined, active, removed, relinquished) 12. As a customer I want to remove a delegate 13. As a customer I want to receive notifications about data product changes 14. As a customer I want to view usage statistics about my data 15. As a customer I want to delete my account to the platform
End User - Delegate	End user - Delegate (type of person) A delegate is a person who is acting on behalf of the customer. 1. As a delegate I want to accept or decline an invite from a customer 2. As a delegate I want to sign up to the platform with my own identity provider 3. As a delegate I want to relinquish my role as a delegate 4. As a delegate I want to view data product of my delegate 5. As a delegate I want to view customer profile details of my delegatee 6. As a delegate I want to view want to see delegatee information 7. As a delegate I want to manage consent of my delegatee 8. As a delegate I want to manage privacy of my delegatee 9. As a delegate I cannot see other delegates of my delegatee
business user - content writer	Business User: Content Writer (type of person) A person who is responsible to write the policy and standards associated with the data product. 1. As a content writer I want to author & manage policies 2. As a content writer I want to author & manage standards 3. As a content writer I want to author divide content into individual sections 4. As a content writer I want to manage the state of individual sections (versions, status) 5. As a content writer I want to re-use individual sections to provide flexibility 6. As a content writer I want to view policy & standards usage 7. As a consent writer I want to invite external collaborators to view and provide feedback on policy 8. As a user I want to see usage statistics
End User – Collaborator	Business User: External Collaborator (type of person) A person that is invited as a collaborator to provide feedback about data products, policy & standards for the purpose of enhancing its content via crowdsourcing from subject matter experts As an external collaborator I want to signup using my own identity provider As an external collaborator I want to view a data product details As an external collaborator I want to view a policy

	As an external collaborator I want to view a standard As an external collaborator I want to provide feedback about data product attributes As an external collaborator I want to provide feedback about a policy As an external collaborator I want to provide feedback about a standard As an external collaborator I want to be notified my registered email

Roles & Responsibilities Hierarchy



Suggestive mock-ups