Data Protection by Design and Default

Executive Summary

The creation and retention of data has increased exponentially over recent years. The introduction of more digital channels has only accelerated this proliferation.

Data is created and moved around as needed, derived data is constantly being generated from original data, itself being on-shipped. Much of this data is stored in vast 'lakes' for analytical purposes.

Organisations have taken advantage of the quantities being collected by putting this data to work in order to learn more about their customers and their habits. Financial crime units also have access to this data for threat mitigation activities.

This pooling of data is complex and has brought them into conflict with different regulatory regimes and jurisdictions, where not all data can be moved or considered in the same way, even for common types. This is principally due to the way that the data was created and to whom it belongs being treated in unique ways.

At a glance

As defined by the ICO:

- The GDPR requires you to put in place appropriate technical and organisational measures to implement the data protection principles and safeguard individual rights. This is 'data protection by design and by default'.
- In essence, this means you have to integrate or 'bake in' data protection into your processing activities and business practices, from the design stage right through the lifecycle.
- This concept is not new. Previously known as 'privacy by design', it has always been part of data protection law. The key change with the GDPR is that it is now a legal requirement.
- Data protection by design is about considering data protection and privacy issues upfront in everything you do. It can help you ensure that you comply with the GDPR's fundamental principles and requirements, and forms part of the focus on accountability.

Privacy Legislation

There is now a plethora of new generation privacy laws around the world. The first and most well-known of these is the Global Data Protection Regulation (GDPR).

It is fully titled Regulation on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

GDPR Summary

GDPR is a piece of unifying regulation intending to strengthen, govern and control the data protection of all individuals within the European Union (EU), including the export of personal data outside of the EU. Primarily it establishes data privacy as a fundamental right, clarifies the responsibilities and a baseline for data protection within the EU and includes the principles for data protection as well as the enforcement powers to compel compliance.

GDPR defines a number of actors in order to explain the concepts of data protection. For the purposes of this document we will need to understand the following: Data Subject, Personal Data, Controller, Processor, Recipient, Filing System and Third Party.

Other Similar Legislation

Following on from GDPR there are a number of other important laws such as California Consumer Privacy Act which can also apply extraterritorially. As such they can interact with each other and care must be taken to apply them properly, especially for multi-jurisdictional companies such as large multi-national financial services organisations.

These obligations can have an impact (as previously stated) on where data can be, who can use it, for what they can use it and finally for how long it is available for all combinations of the above. Typically, the function of creating the policy for this cross-cutting concern falls to a compliance-type department.

The enforcement of the policies themselves is an operational task and is usually quite manual. New, automated, data sharing frameworks are a concept that enshrine the need to be more agile, mechanical and to move away from the manual burden of legacy understandings of how to control data.

To ensure the new frameworks remains robust, relevant and up-to-date, the usage of appropriate tooling is required to facilitate the effectiveness of this framework and future scalability. The strategic solution is to “digitise” the data sharing agreement contractual frameworks with the ability to produce process outputs (eg, automated approvals) to users and connecting applications ensuring the participation of the relevant stakeholders in real-time.

In order to digitise and lift the meaningful information from the contracts, Solidatus offers the ability to provide a platform where not only inputs can be uploaded, eg, terms and conditions, but also to map meaningful relationships which can be codified into the metadata and a query language.

This allows the organisation to streamline contractual, legal and regulatory compliance requirements, reduce the documentation that needs to be completed and executed for each project. Also, to take a more holistic, group-wide view of data sharing while remaining compliant with applicable laws and regulations.

All of this is linked to the underlying purposes for which data is shared, the sub-processes related to those purposes and the data categories related to these. This provides a real time view of what restrictions apply to existing processing.

An Example Output

A model should be built which encompasses the following components:

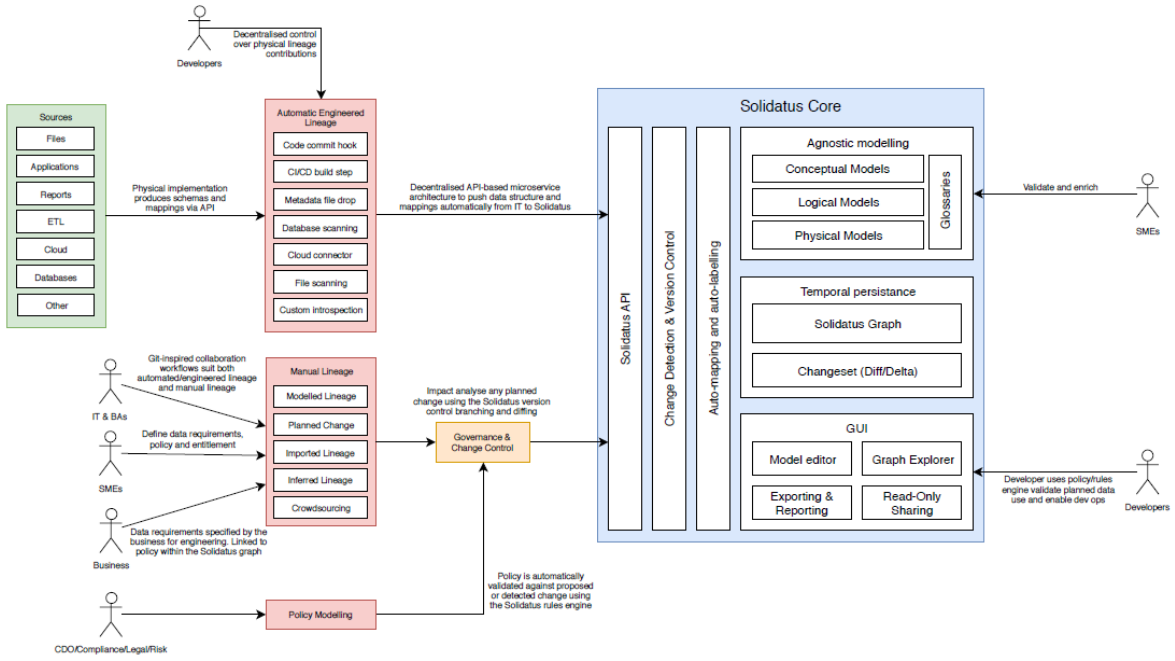
1) External regulations (eg, GDPR, India Data Protection Bill, CCPA, Malta Data Protection Act)
2) Organisational components (eg, list of data privacy controls, operating countries and entities)
3) Data sharing agreement (including all Schedules and Appendices)
4) Compliance inventory (Purposes, Processes), Data Categories and Data Subjects
5) Relationship map and metadata library, so the model can be queried showing traces and impact across all joint processes (from regulations, data sharing and all the way to data category attributes)

As such, this can prove to be a very powerful output, which can immediately tell the user which countries participating in data sharing agreements, on what conditions, which processes and data categories is impacting and even which external regulations are driving the impact with a few clicks of the button.

Benefits

- Provides capability to digitise complex policies and map to multiple other organisational processes as well as external influencers (eg, regulations)
- Immediate outcome reports and traceability
- Ability to assess the impact of future change, eg, if a new data privacy regulation comes into effect, we are able to map its impact to our organisational processes
- No content is being "overwritten", instead a new fork is being established every time there is any change within the model or a relationship. This allows full auditability and transparency and can provide a "real-time" snapshot of the organisational policies at play historically
- The interface is very user friendly, and adaptable
- Require limited resources to maintain a solution
- It has a capability to integrate with other applications within organisation and provide reporting and multiple outputs mechanism
- All metadata can be "codified" and managed through query language

Solidatus - Metadata Development Lifecycle in a
Flow Enabled Organisation Centralised Control – Decentralised Execution



About Solidatus

Solidatus is a leading data lineage, business relationship and conceptual modelling tool that enables the effective management of data, people and processes. It has solidified its place as one of the most influential and critical new software solutions positioned to help the world's largest data-rich and regulated organisations manage their processes and data. It highlights gaps, declares transparency and provides a simpler, quicker and better route to implement change.

Solidatus facilitates both data lineage and business process engineering. Whether to demonstrate regulatory compliance, improve governance, assist with transformational change or reduce inefficiencies in data handling, it is uniquely engineered to build end-to-end data models more efficiently and

effectively and improve an organisations data economy. Solidatus is quickly being adopted by organisations across the globe, including top-tier global financial, pharmaceutical, utility and infrastructure firms and has been implemented by leading consulting and technology firms.