Swiss Data Custodian

White Paper

Privacy Protection in a Data-Driven Economy

Data plays a critical role in today's economy. The EU is currently developing data spaces to create a *data market* where data can be exchanged, sold, and utilized for various objectives, including training algorithms in medicine and other industries. In this data-driven economy, safeguarding personal data is a crucial issue that must be tackled by all stakeholders.

The EU established a legal framework for data privacy in 2018 through the implementation of the General Data Protection Regulation (2016/679). Since then, non-compliance with data privacy regulations has become a criminal offense, punishable by substantial fines. Individuals must now provide consent for each specific use case of their data and have the right to request its deletion or retrieval in certain circumstances. Despite not being part of the EU, markets are interconnected, and EU laws often set the standard for privacy protection globally, including in Switzerland. The new Federal Act on Data Protection (nFADP), which takes effect on September 1st, 2023, aligns with European laws while offering additional flexibility for data processing outside the scope of the GDPR. However, it also contains provisions that are more stringent than the GDPR.

It is imperative for organizations participating in the data market to ensure compliance with privacy regulations. However, this can be a challenging task, requiring the ongoing collection of consent for data usage and continuous monitoring to ensure compliance. This highlights the need for a specialist solution to handle privacy protection effectively. Introducing the *Swiss Data Custodian*, an application that offers a solution to this problem. With its ability to easily integrate into existing systems, the Custodian takes care of privacy protection, freeing businesses from the burden of monitoring data usage and compliance and allowing them to focus on building their business case.

“The Swiss Data Custodian is a human-centric and trustworthy solution for digital privacy compliance.”

Swiss Data Custodian

The Swiss Data Custodian is an open-source framework developed by the Swiss Data Science Center, that provides the necessary tools to govern data access and processing, and enables secure and compliant data usage through contractual agreements. It incorporates existing technical standards for data formats and interfaces to guarantee interoperability in existing ecosystems.

One of the core goals of the Swiss Data Custodian is to empower data subjects with the tools they need to provide informed consent for data collection and processing. The Custodian has a more nuanced approach to consent, allowing data subjects to clearly express their preferences and control their data usage. The framework also enables the auditability of consent and ensures that its execution does not conflict with relevant regulations.

The Custodian enforces privacy and security regarding data accessibility and disclosure with trust-based data governance that maintains compliance with data regulations.

Finally, the Custodian provides transparency and auditability throughout the data access and processing lifecycle. It ensures that data is processed in a secure and compliant way.

Trusted Health Data Sharing Use Case

In elite sports, it is critical to take measurements of performance during training sessions and competitions. Collecting athletes' health data provides measures for factors such as fitness level and heart rate recovery. Many parties and sources are involved in this data collection and analysis over different periods and locations. The whole picture of the athlete's health record can benefit all involved health professionals. Nevertheless, this data is hard to access without the athlete's consent. In this use case, we integrated the Custodian with an existing health data platform where the health professional can request athlete's data access and processing. The Custodian enables the athletes to give and revoke their consent to make their data accessible. The athlete can also monitor data access and process requests and activities done by health professionals.

User Contract Manager

The Custodian handles contracts for data access and processing. A contract encapsulates contractual terms, contractors' information, and data access and processing policies. It is available in a human and machine-readable format. The Custodian provides a User Contract Manager, which automates the contracting process between data providers and consumers. Two contract types can be created and processed by the User Contract Manager:

- A B2B contract, which refers to the contract between organizations that want to set up data sharing and processing agreements.

- A B2C contract, which refers to consent between a service provider and a data subject. The data subject must agree to, and sign the consent clause to obtain services from the service provider. Furthermore, it is possible for a data subject to create consent for personal data sharing without the need to consume services. For example, data subjects might want to participate in an experiment by sharing personal data. In both cases, the data subject can express some restrictions in the consent.

Contract Lifecycle

1. **Generate Contract Template.** This initial stage is about the creation of a contract template that specifies contractual terms and policies on data sharing and processing. In some cases, the contract can be autogenerated based on the requirements of the data provider. The contract can also be generated based on an existing contract, mapped to a standardized version of the contract template provided by the Contract Manager System. Finally, the contractual parties can edit the terms of the contract.
2. **Validate Contract**. In this stage, the contract is verified to assess its compliance with regulations and standards requirements.
3. **Sign Contract**. Once reviewed and approved, the contract is put out for signatures for all parties via digital signature with digital certificates.
4. **Execute contract.** After signature, the contract is deployed and executed by notifying the data governance component, which triggers the data sharing and processing workflow. During the contract execution, the data sharing and processing activities are tracked to meet the contractual obligations. A monitoring workflow triggers alerts and notifications when there are suspicious activities. The contractual parties are notified during the contract stages.
5. **Terminate or Renew Contract**. The termination or renewal stage handles the contract's status determining whether it will be terminated or renewed.

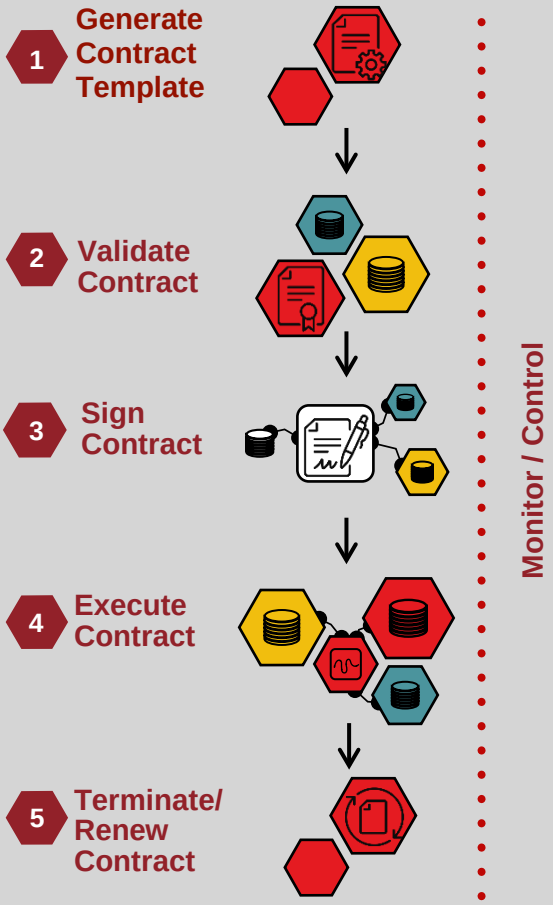

Figure 1 - Contract lifecycle

Governance of Data Access and Usage

Data access and usage governance refer to how permission is granted or denied for data access and processing. The Custodian provides a governance building block based on the Attribute- Based Access Control method with the main components described below.

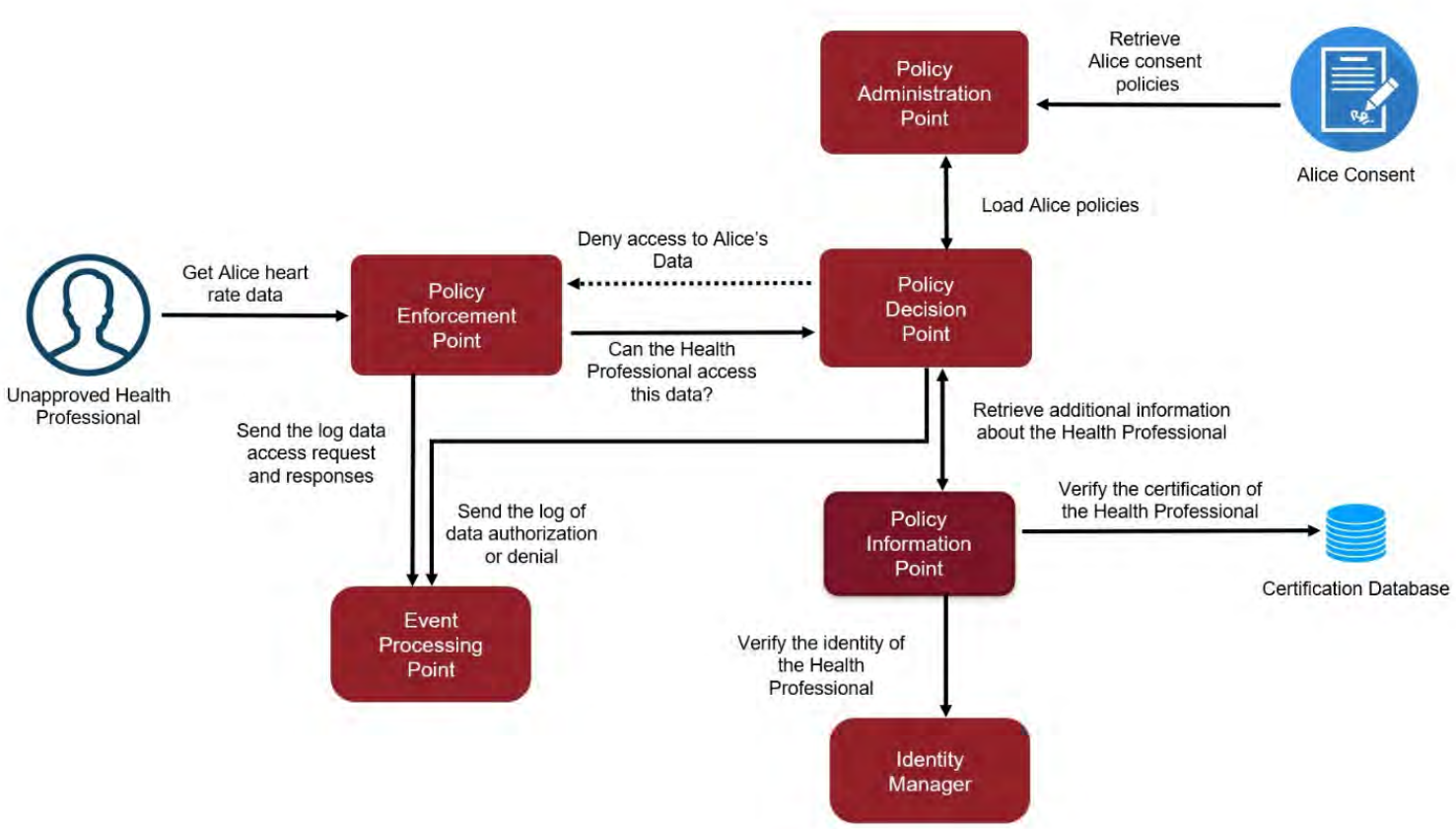

Figure 2 - Main components of the data access and usage governance

Policy Administration Point

The Policy Administration Point is the interface for creating data access and privacy policies for data access and processing. It extracts these policies from a contract.

Policy Information Point

The Policy Information Point provides missing information called *attributes* during the policy evaluation. For example, an attribute such as "*a licensed health professional*" may be requested to obtain an athlete's medical record. The Policy Information Point retrieves and fetches this information from an authorized source.

Policy Decision Point

The Policy Decision Point receives the incoming requests for data access and processing from a Policy Enforcement Point. Then, it applies the corresponding policies from the Policy Administration Point to the request, allowing or denying access. The Policy Decision Point also uses some contextual information from the Policy Information Point for decision-making.

Policy Enforcement Point

The Policy Enforcement Point presents incoming data access requests from a data consumer to the Policy Decision Point. A data access and processing request has different attributes, such as the data consumer identity, the data asset, and the purpose of the data processing. It is also responsible for delivering the final permission or denial of data access and processing to the data consumer.

Event Processing Point

The Event Processing Point monitors the events generated by the User Contract Manager, Policy Decision Point, and Policy Enforcement Point. It represents an audit mechanism to create evidence of data access and processing compliance. For instance, through the Event Processing Point, data subjects have full transparency of the lineage of their data, how it is being accessed, by whom, and for what purposes.

Identity Management service

The Custodian includes a local Identity Management service that can be integrated with External Identity Management services.

Technical Implementation

The Swiss Data Custodian follows a micro-services architecture pattern in which all components are independent processes that interact through messaging. The services are configurable and can be combined depending on the use cases. Internal service communication is achieved asynchronously via message queues. The User Contract Manager and the Policy Enforcement Point functionalities are exposed to other systems and front-end callers via REST endpoints. The contracts are formatted in JSON schema and securely stored in a document database. The JSON schema provides a standardized definition of the contract terms, while the document database ensures efficient contract storage and retrieval.

Future development

The Swiss Data Custodian project is constantly evolving and progressing. New features enhance its key components and ensure that it continues to meet evolving privacy protection requirements. Exciting new developments include:

- A *knowledge graph-based tool* to verify contract compliance with privacy regulations such as GDPR and nFADP. This tool will carefully scrutinize contract policies to prevent inconsistencies and ensure parties adhere to the rules.
- The implementation of *privacy-based access control* to adapt the management of data access and use based on the privacy policies. The policies will determine the level of access to data and the specific ways in which it can be used.
- *Privacy-preserving plugins*, such as data encryption at the Policy Enforcement Point, will add more privacy and security to the data. These plugins, potentially coordinated by trusted third-party services, will further ensure the confidentiality and protection of the data for all parties involved.