ANNEX V-A

Consent Building Block Specifications

1. Description

The Consent Management Building Block enables services for individuals to approve the use of their personal data by defining the principles, functions and architecture of an information system. For organizations that process personal data,it provides the ability to know the individual's will and legitimately process such personal data.

The Consent Management Building Block is a process-oriented GovStack Building Block facilitating auditable bilateral agreements within a multi-agent environment that integrates with most other BBs.

This specification has used several available and recognized open standards below and legal frameworks (such as the GDPR) for laying the groundwork for its approach to consent management. :

- Kantara Initiative - Consent Specification
- ISO 29184: 2020: Online Privacy Notices and Consent
- ISO/IEC 29100:2011: Privacy framework
- ISO/TS 17975:2015 Health informatics — Principles and data requirements for consent in the Collection, Use or Disclosure of personal health information
- ISO/IEC TS 27560 — Consent record information structure (under development)

1.1 What Consent is

In the GovStack context, consent is understood as a voluntary declaration by an individual to approve the processing of their Personal data. It is one specific justification for personal data processing that is assumed to be required by legal or ethical conditions. It assumes that the person can decide on processing their personal data, managed in and by other GovStack BBs, and that they are free to withdraw their consent at any time.

1.2 What Consent is not

The use of *consent* should be avoided in cases as below, which are not part of this specification:

- When a person is simply informed of the processing of the data by the organisation as part of the service provided under contract or by an authority.

- When consent does not have to be obtained in a situation where the entity does not identify or cannot identify people with reasonable effort.

1.3 Terminology

Term	Description
Configuration	technical implementation of all the content and process conditions as defined by the Data Policy for Consent Agreement creation, reading, updating and deletion, as well as for providing all necessary actors with the required operations
Consent Agreement	is the agreement to be signed by the Individual and the Data Controller as prescribed by Data Policy, based on which the Data Providing System may transmit the data to the Data Consuming System for the purposes described in the Consent Agreement.
Consent Record	is created when an individual signs a consent agreement. It represents a signed consent agreement.
Consent Reference	a unique identifier used to locate and verify the validity of the Consent Agreement.
Data Providers	is a legal entity that stores and provides access to an Individual's data, which requires the Individual's consent for processing (outside of its primary purpose/location).
Data Consumers	is a legal entity that requires the Individual's data from the Data Providers according to the consent of the Individual.
Data Disclosure Agreements	A Data Disclosure Agreement (DDA) exists between two organisations where one organisation acts as a Data Provider and the other as a Data Consumer. The DDA captures how data is shared between the two organisations and each party's role and obligation.
Data Policy	is a formal description of the purpose, nature and extent of consent-based personal data processing, covering the configuration needs by Data Providing System and Data Consuming System and the conditions defined by law.
Data Processing Auditor	is an entity (a person or an organisation) verifying the legitimacy of personal data processing by Data Controllers and Data Processors based on the Data Policies and performed tasks. The entity is not to be confused with a data policy auditor that is independent of the actors involved in the operations of consent management and can engage directly with the Consent Management service operator.
Delegate	the person giving consent (signing Consent Agreement); on behalf of the Individual,
Individual	is a person about whom the personal data is stored in an information system (a.k.a. "Data

Term	Description
	Subject") and who agrees or not with the use of this data outside of its primary purpose/location.
Legal Entity	is an organisation (public or private) that has the rights and obligations to define standards for personal data processing. E.g. a public health authority
Personal data	Is any information that (a) can be used to identify the Individual to whom such information relates, or (b) is or might be directly or indirectly linked to the Individual (ISO(IEC 29100:2011)
Regulations	are broadly defined as rules followed by any system: could be laws, bylaws, norms or architectures[1] that regulates a given system.

1.4 Consent Agreement Lifecycle

The life cycle of consent management starts and ends within the organisation responsible for the information system. The organisation knows the context in which the information system operates and the intended purpose of the service. The rules and regulations to be applied for a given level of assurance define the functional framework for consent management.

Consent BB deals with transparency on data usage in a given context. Thus privacy-by-design of the system's actors is often an excellent guiding principle for interpreting international, national and organisational policies and governance principles to implement the functional consent framework. A tangible outcome from a data protection impact analysis (DPIA) is a structured approach that can deliver the input for the actual implementation of the Consent BB.

Individual consent is captured within the context of digital interaction. This interaction is composite of all the information systems involved, not solely Consent BB. Thus, the legal and ethical boundaries of consent are defined in the entirety of the interaction. In particular, consent, as defined by ISO/TS 17975:2015(E), should be seen as a "set of agreements and constraints" that an informed and knowledgeable [individual] agrees to apply to their data processing. This definition, not based on the purpose of the data usage, can lead to a consent management framework incorporating authorisations or unrelated constraints of the system. For example, in health information and healthcare service delivery, consent is also the process whereby a set of constraints is agreed upon so that information may be collected, used, or disclosed. However, it is also the outcome of the process. As a rule of thumb, limiting unintended secondary usage of data is helpful to separate "consent" for a purpose from "consent" as an agreement to constraints and authorisation imposed by the system's functional requirements.

[1] Defintion inspired by Lessig's modalities of regulation: https://lessig.org/images/resources/1999-Code.pdf

As a result, the organisation responsible for the information system is the driver of the definition of the functional consent management framework. It is also the function of the organisation to design the workflow for obtaining and processing the consent in a purposeful but not annoying for individuals or data processors with unnecessary bureaucratic overhead. From this framework, the Consent Building Block achieves its purpose by employing Consent Agreements that contain the following:

- A data policy that could be reused across multiple consent agreements (for example, based on GDPR or any specific regulation)
- The purpose of consent, processed data attributes
- Signatures

A consent agreement life-cycle has four main phases[2], as illustrated in the figure below:

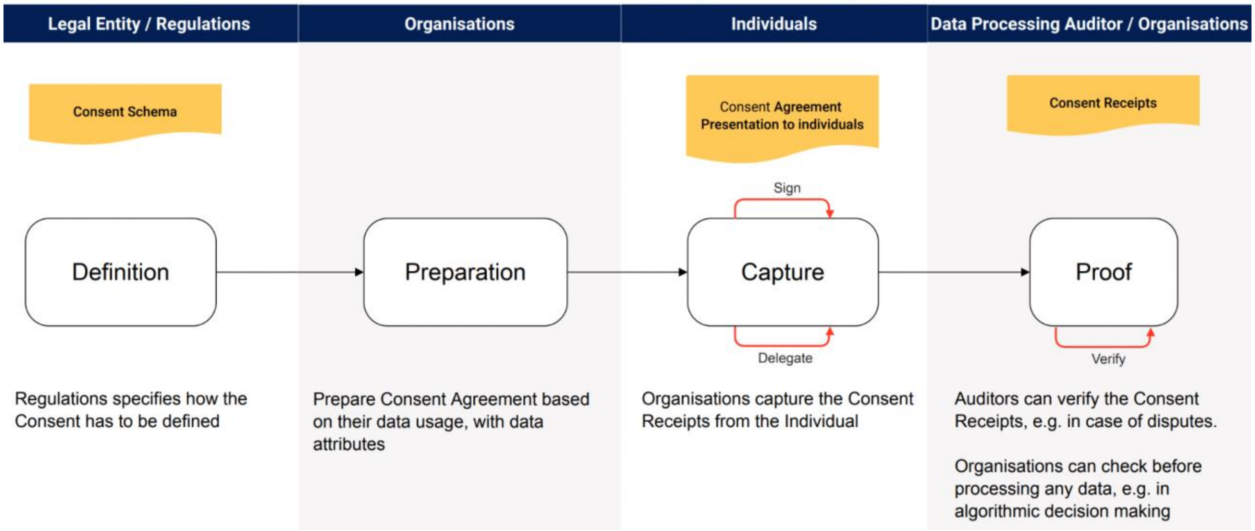
Legal Entity / Regulations
Organisations
Individuals
Data Processing Auditor / Organisations
Consent Schema
Consent Agreement Presentation to individuals
Consent Receipts
Sign
Definition
Preparation
Capture
Proof
Delegate
Verify
Regulations specifies how the Consent has to be defined
Prepare Consent Agreement based on their data usage, with data attributes
Organisations capture the Consent Receipts from the Individual
Auditors can verify the Consent Receipts, e.g. in case of disputes.
Organisations can check before processing any data, e.g. in algorithmic decision making

Diagram Source

Definition: In this phase, the organisation (a Data Provider or a Data Consumer) adopts and defines a Data Policy that applies to the industry or sector-specific data usage as a template. While this phase is considered a “black box” to the Consent BB, it is an essential reference point for configuration and compatibility checks in all following phases.

Preparation: In this phase, the organisation (A Data Provider or a Data Consumer) that intends to process personal data configures the Consent Agreement and relevant rules for its use. An organisation could use personal data for third-party data sharing, for example.

Capture: In this phase, the Individual can review the Consent Agreement and, once agreed, it is captured in a Consent Record by the organisation and stored for verification. This allows an auditor to check and ensure

[2] Inspired from similar work done by NGI eSSIF-Lab ADA Project Data Agreement Specification.

records are in place to process the individual's personal data. In future, this phase could also encompass delegation and other individual use cases.

Proof: In this phase, an organisation (A Data Provider or a Data Consumer) can demonstrate that a valid record exists for performing data processing within itself or with other organisations. This allows for internal usage and for an auditor to verify and ensure records are in place to process the individual's personal data.

1.5 Actors

The following actors (performing a distinct human role) are identified to be acting on the Consent BB.

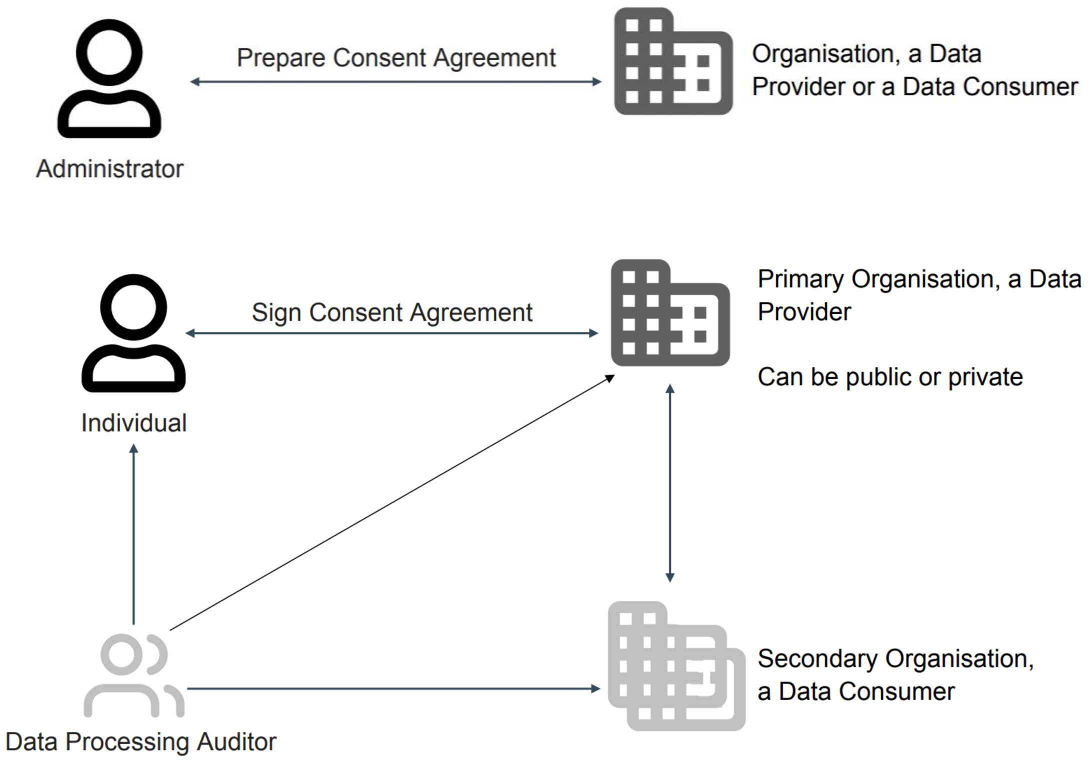
Prepare Consent Agreement
Organisation, a Data Provider or a Data Consumer
Administrator
Sign Consent Agreement
Primary Organisation, a Data Provider
Can be public or private
Individual
Secondary Organisation, a Data Consumer
Data Processing Auditor

Diagram Source

1.5.1 Individual

The capabilities for individuals that Consent BB supports are:

- viewing and understanding Data Policies applying to their personal data processing;
- agreeing and disagreeing with and toggling between the conditions of personal data use as described in the Consent Agreement;
- obtaining copies of their Consent Agreement(s);
- delegating their consent rights (out-of-scope for current technical release)

The scope for version 1.0 of Consent BB assumes that the Individual is acting for her-/himself. Ultimately the Consent BB will include in the Consenting Process the capacity to sign a Consent Agreement in the name of another individual - to act as the Delegate, which is used as the criterion for technical implementation. However, the Delegate and the Individual relationship is expected to be maintained outside of the Consent Manager, which assumes that the person signing the Consent Agreement (i.e. Consenter) has been authorised to do so.

1.5.2 Administrator

The Administrator (Data Provider or Data Consumer Admin) configures the consent management system on behalf of the organisation. The main actions expected to perform via Consent BB are:

- configuring Data Policies, requesting and signing Consent Agreements with Individuals;
- viewing (reading, exporting) the Consent Agreements and relevant reports;
- event-driven (opt-in or opt-out) subscription to (notifications of) changes in Consent Agreements;
- logging and maintaining an auditable overview of all personal data transactions according to Consent Agreements as well as configuration versions.

1.5.3 Data Processing Auditor

The main action a Data Processing Auditor (or Data Protection Officer, DPO) is expected to perform via Consent BB are:

1. auditing tracking the consents (opt-in/opt-out);
2. auditing tracking Data Policy changes and configuration conformance with it;
3. viewing (reading, exporting) the Consent Agreements and relevant reports in a verifiable form.

The Data Processing Auditor relies on an audit universe defined by the control and risk management of the specific project and context (i.e. outside the Consent BB). "*Who needs to consent to what*" is the outcome of a DPIA (Data Protection Impact Analysis), ensuring that the data policies comply with the project's relevant data protection regulations.

For implementing a specific use case, it is important to distinguish the Data Processing Auditor, an actor described here, from a data policy auditor, an actor of the risk organisation. The two roles are expected to be coordinated in the risk management process. Within the Consent BB, the Data Processing Auditor performs the tasks that will allow a data policy auditor to confirm that the implemented system complies with existing regulations demanding consent.

2 Key Digital Functionalities

Consent BB enables the organisations to enforce Data Policies that require signed consent by Individuals for the use of their personal data. Its key purpose is to allow individuals to view Consent Agreements and sign or withdraw their consent on what personal data is used and accessible to organisations. It also clarifies the Data Policy applied, such as the purpose, retention period, jurisdiction, third-party data sharing, etc.

The Consent BB implements the key functionalities described in the consent management lifecycle. It includes the ability to configure consent agreement by an organisation admin, present consent requests towards individuals, capture consents, enable queries if consent exists or not, and enable independent audit of consents.

2.1 Assumptions

This lays out the pre-conditions needed for anyone to use Consent BB.

1. Data Disclosure Agreements between organisations are already in place. For e.g. a healthcare organisation has already been authorised to use the citizen data registry.
2. To link a Consent Agreement with the specific Individual, Consent BB assumes the authentication & authorisation to be handled in a trusted manner outside of it (see below).
3. Within the early scope of the Consent BB, the act of delegating is kept outside the scope of Consent BB. It is assumed that the authorisation to act on behalf of someone else is already resolved.
4. It is the organisation's (a Data Provider or a Data Consumer) obligation to manage and implement internal policies towards its employees relating to their individual responsibilities for Personal data processing integrity, specifying it in the employment contract or by other means.

2.2 Out of Scope and Future Considerations

The following use cases are out of scope for this version 1.0 of Consent BB. These may be considered as potential future enhancements.

1. Non-reusable/single-action consent given in physical settings.
2. Consent to use data other than personal information on behalf of an organisation. For example, an organisation authorising an individual to consent to expose some organisation's data is seen out of the scope of the consent building block.
3. Consent delegation: While part of the Consent BB, this will be taken up in the future. For e.g. an individual is authorising another individual to consent on their behalf.
4. "Multi-Consent" is when consent can be given by more than one person or consent is required to be given by more than one person. An example is given by the registration of a child whose consent is actually given by a parent or both in certain use cases.
   In the current version of the specification, muti-consent can be implemented at the business process level, with multiple calls to the Consent BB. One call per consent transaction. In the future, it is planned to extend the functionalities of the BB to provide support for multi-consent.
5. Relationships between multiple Agreements will allow for a single transaction to capture an individual's signature on multiple Agreements.
6. Consider individual rights (E.g. as per GDPR / Data Protection Act etc.), potentially amending Scenarios 4.x, API endpoints functionality and the capture of Consent Records.

   a. The right to be informed
   b. The right of access
   c. The right to rectification
   d. The right to erasure

e. The right to restrict processing

f. The right to data portability

g. The right to object

h. Rights about automated decision-making and profiling.

7. The elaborated lifecycle for Consent Agreement amendments: Data Policies and Consent Agreements may change over time. Such events are sensitive to existing Consent Records.

   a. Notifications for any consent agreement changes; Individuals and Data Consuming and Data Providing Systems.

   b. Notifications of Consent Record changes in bulk and separate: Data Consuming and Data Processing Systems.

   c. All lifecycle events of Consent Agreements and Consent Records are mapped as Audit Event Types, and the external auditing system is notified.

8. Roles and scopes for IAM (Identity Management) and RBAC to be used within consent BB
9. We need to enable audit logging capabilities aligned with the overall GovStack goals. Issues to be addressed include audit log access control, the type of information captured in the audit log, and taking care of sensitive data or meaningful metadata.
10. Certain update use cases (e.g. modify consent agreement) might result in invalidating a previously acquired individual consent. This will be investigated for future releases.

2.3 Consent BB Components

Within **the scope of Consent BB version 1.0,** the required components are as given:

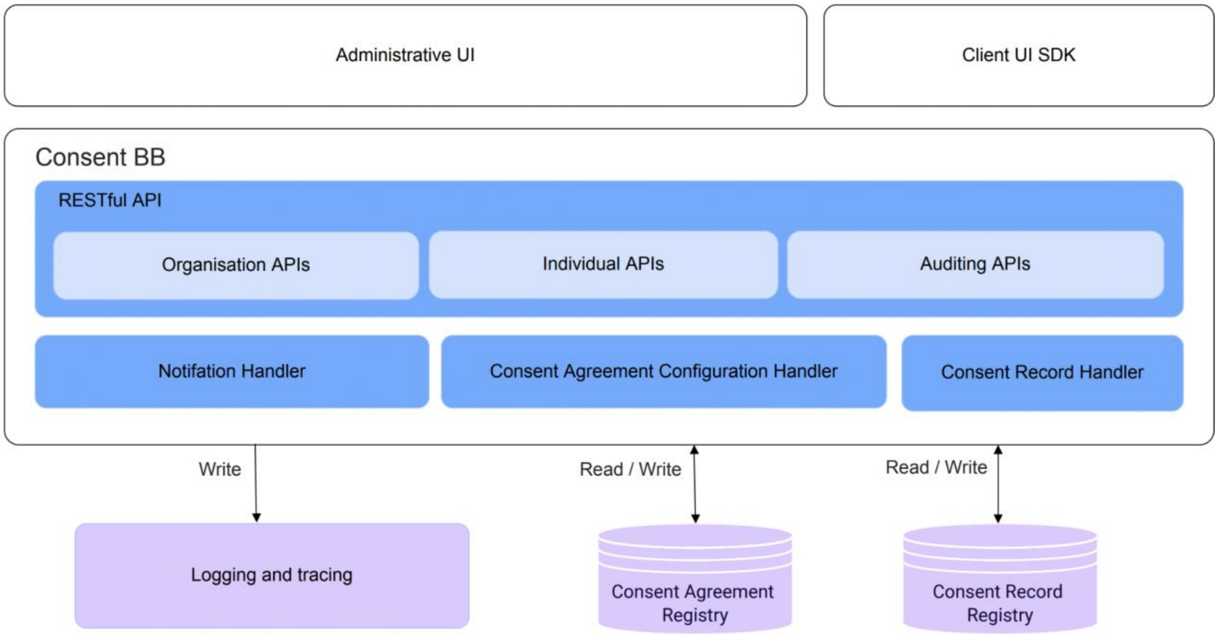

Diagram Source

Consent Agreement Configuration Handler - handles the creation, updation & deletion of consent agreements for organisations. Organisations can be Data Providers or Data Consumers

Consent Record Handler "enables Individuals to view data usage and consent record.

Notification Handler: Handles all notification configurations and notifications requested by different subscribers.

Administrative UI and client UI SDKs: These are readily available components that can configure and use the services offered, making integration easy and low code.

RESTful APIs: All APIs are exposed as RESTful APIs. These are categorised into Organisation APIs, Individual APIs and Auditing APIs.

2.4 Interaction with other Building Blocks

The overall relationship diagram is shown below.

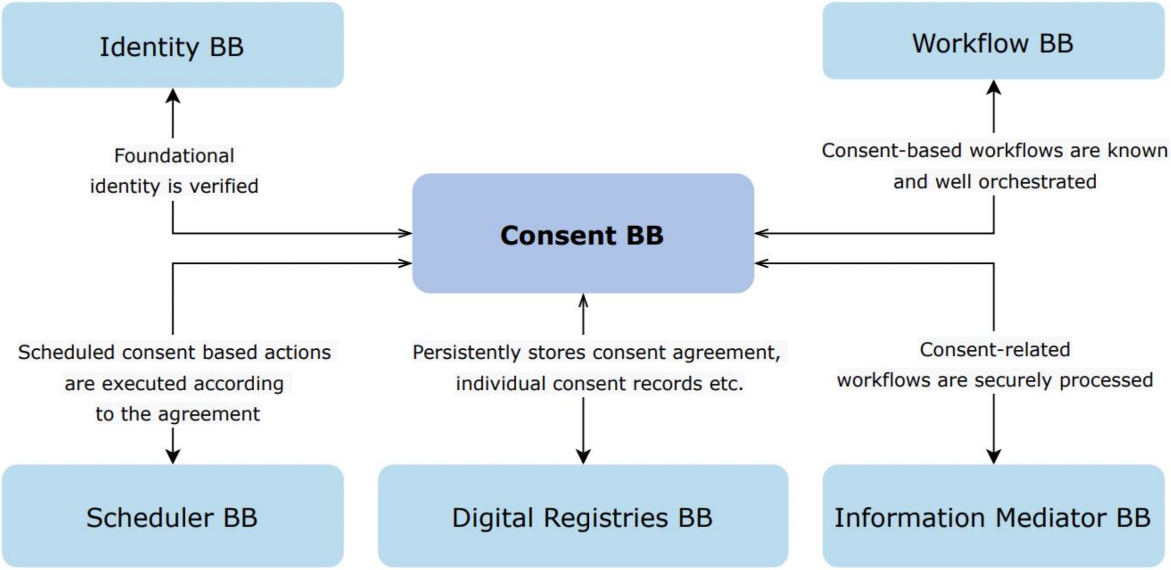
Identity BB
Workflow BB
Foundational identity is verified
Consent-based workflows are known and well orchestrated
Consent BB
Scheduled consent based actions are executed according to the agreement
Persistently stores consent agreement, individual consent records etc.
Consent-related workflows are securely processed
Scheduler BB
Digital Registries BB
Information Mediator BB

Diagram Source

The table below summarises the key relationships consumed during a consent transaction.

Building Block	Relationship description
1. [Identity BB]	It is assumed the Consent BB has already obtained requisite access tokens
2. [Digital Registries BB]	This is used to store any consent agreement, individual consent receipts etc.

Building Block	Relationship description
3. Workflow BB	Manages the workflow and rules associated with requiring or not requiring consent to use personal data.
4. Scheduler BB	Provides an engine for time-based triggers to various events of an automated business process, which might also require consent.
5. Information mediator BB	The information mediator BB provides a gateway for exchanging data related to consenting workflows; it also provides logs for auditing purposes.

2.5 Universal Consent Workflows

The workflow BB triggers the need for consent as part of the general business flow. The assumption is that a consenting process never exists outside of a purposeful comprehensive business process. Hence, it is important to define and control the data processing activities as part of a holistic data service. This section lays out key universal consent workflows that can be re-used within the various use-cases (see explanation in Workflow BB). This enforces the best practices for organisations to adhere to personal data processing standards in any given context and jurisdiction. In these sequences, we have removed the Digital Registries BB in the sequence for simplicity. It will store all persistent consent data.

2.5.1 Consenting at initial registration (Pre-registration) using a centralised ID system

The first and somewhat unique use-case is related to the need for consent when the Individual is not yet provisioned in the System processing the data. In such cases, the workflow requires the creation of a valid and trusted Foundational ID to be linked with the Consent Record. Below is shown how a pre-registration use of consent workflow works.

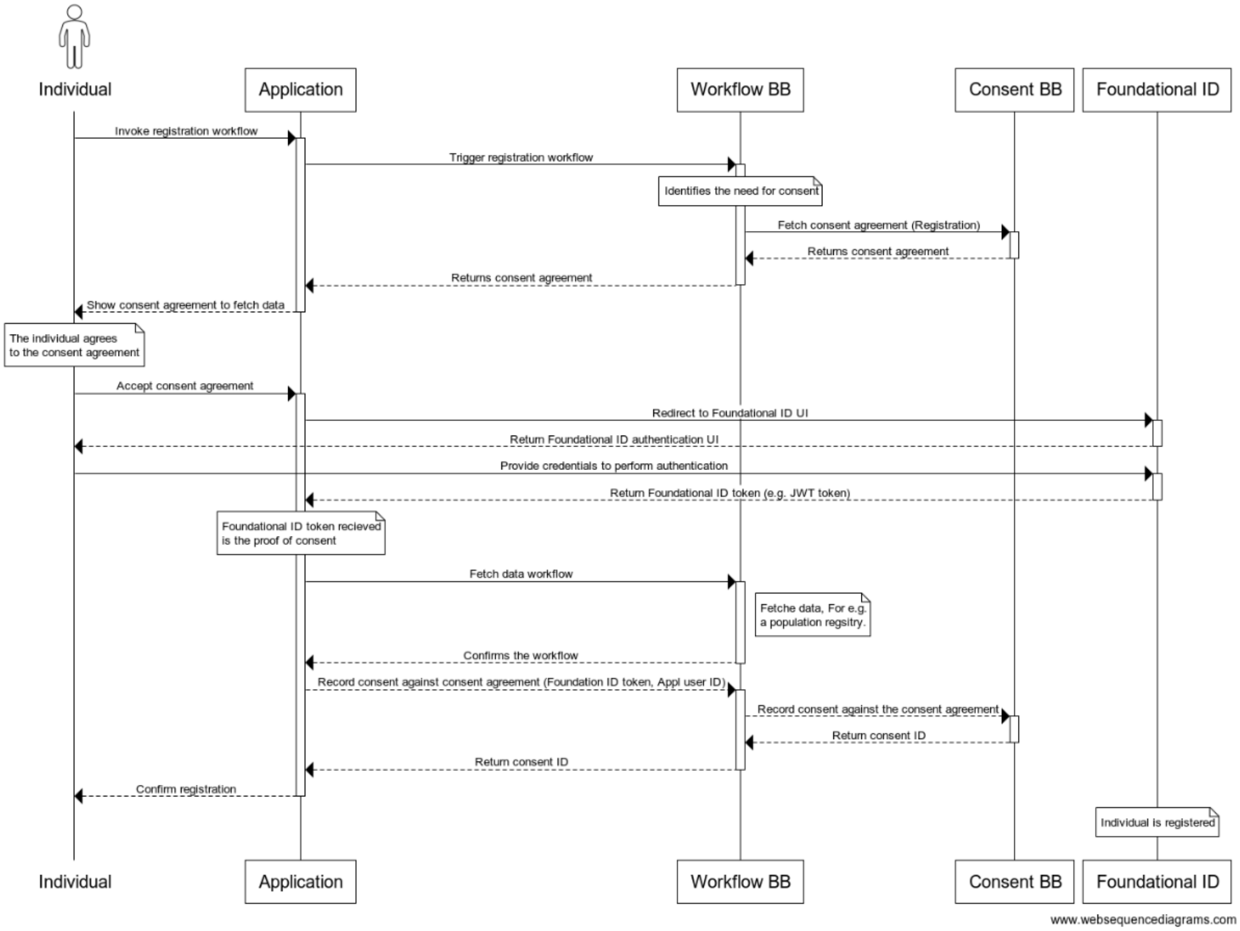
Individual
Application
Workflow BB
Consent BB
Foundational ID
Invoke registration workflow
Trigger registration workflow
Identifies the need for consent
Fetch consent agreement (Registration)
Returns consent agreement
Returns consent agreement
Show consent agreement to fetch data
The individual agrees
to the consent agreement
Accept consent agreement
Redirect to Foundational ID UI
Return Foundational ID authentication UI
Provide credentials to perform authentication
Return Foundational ID token (e.g. JWT token)
Foundational ID token recieved
is the proof of consent
Fetch data workflow
Fetche data, For e.g.
a population regsitry.
Confirms the workflow
Record consent against consent agreement (Foundation ID token, Appl user ID)
Record consent against the consent agreement
Return consent ID
Return consent ID
Confirm registration
Individual is registered
Individual
Application
Workflow BB
Consent BB
Foundational ID
www.websequencediagrams.com

Diagram Source

2.5.2 Consenting after the registration (Post-registration)

In more frequent situations, when the Individual is already provisioned in the System (post-registration), the consent workflow use the existing ID tokens, and only the Consent Record is to be created. The following diagram shows how a generic post-registration use of consent works:

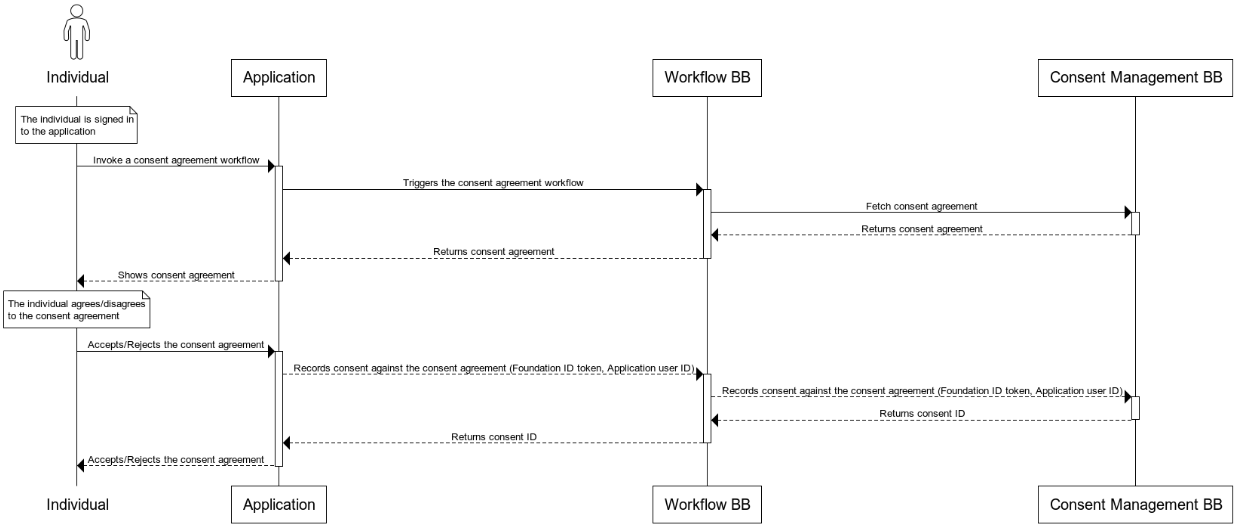
Individual
Application
Workflow BB
Consent Management BB
The individual is signed in to the application
Invoke a consent agreement workflow
Triggers the consent agreement workflow
Fetch consent agreement
Returns consent agreement
Returns consent agreement
Shows consent agreement
The individual agrees/disagrees to the consent agreement
Accepts/Rejects the consent agreement
Records consent against the consent agreement (Foundation ID token, Application user ID)
Records consent against the consent agreement (Foundation ID token, Application user ID)
Returns consent ID
Returns consent ID
Accepts/Rejects the consent agreement
Individual
Application
Workflow BB
Consent Management BB

Diagram Source (Revised)

2.5.3 Consent Verification

The third universal workflow is about verifying if a valid Consent Record exists or not for a given data processing event within a business process. This may be the immediate continuation of a consenting workflow by the same System that acquired the Consent Record, or it may be used by a separate business process by a different Application or at a different time. The same verification workflow may also be used for auditing purposes. The following diagram shows how a generic verification for valid consent works:

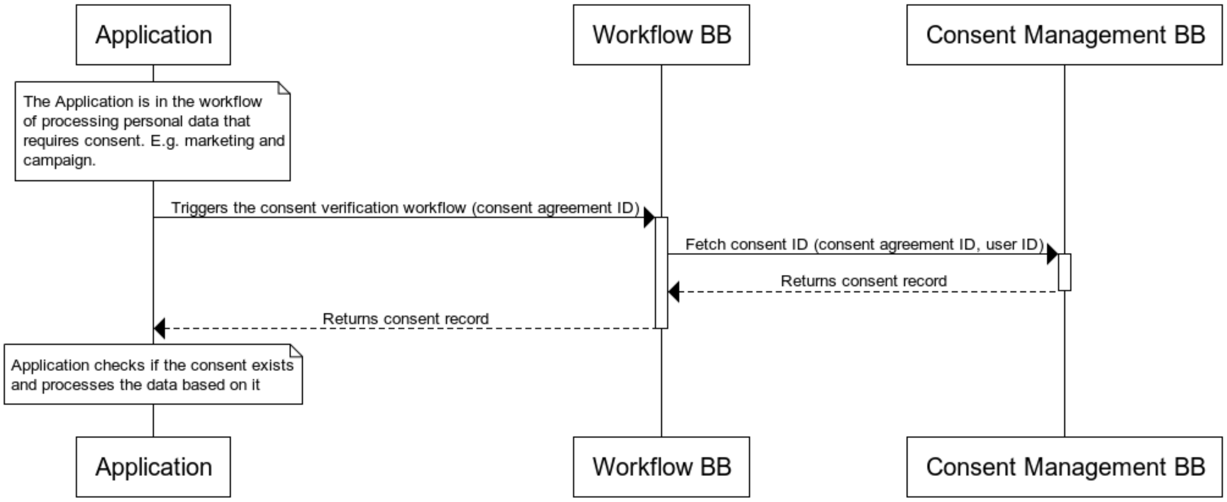
Application
Workflow BB
Consent Management BB
The Application is in the workflow of processing personal data that requires consent. E.g. marketing and campaign.
Triggers the consent verification workflow (consent agreement ID)
Fetch consent ID (consent agreement ID, user ID)
Returns consent record
Returns consent record
Application checks if the consent exists and processes the data based on it
Application
Workflow BB
Consent Management BB

Diagram Source (Revised)

2.6 Functionalities

The functionalities are derived from the consent agreement lifecycle and categorised according to the Actors described above. While the consenting workflows (as described above) are implicitly considered the centrepiece of Consent BB, it is important to realise that the integrity of consent management can only be achieved if robust configuration before and auditing after the Consent Agreement signing and Consent Record verification activities are in place. Hence, the functionalities are described following the logical sequence of the consent agreement lifecycle, and they are all equally important components of the Consent BB.

The consent process (creating and signing Consent Agreements and Consent Records) is initially managed in the application provided by the Organisation that is legally required to collect the consent. Since it can be either a Data Consuming organisation or a Data providing organisation, the Consent BB allows both to verify their conformance with the underlying Data Policy, both organisations must be able to access and use the application.

While the Actors generally fall in line with the categories of the functionalities, it is important to realise that “auditing” functions in the narrow sense - verifying if data processing is being (or has been) processed according to the Data Policy requiring a consent - is relevant to various entities involved in the data processing. For this reason, the generic “verification” activity may be executed as part of various workflows satisfying the needs of different actors.

2.6.1 Administrator User Functionalities

The table below summarises the key use cases identified for an organisation's Administrator. Organisations can be Data Consumers or Data Providers, i.e. the organisations legally delegated the responsibility for collecting consent for the systems handling personal data processing.

It is foreseen that one organisation involved in the data processing transaction takes responsibility for the configuration of Data Policy and respective Consent Agreements(s), and so the organisation’s Administrator maintains the required configurations.

Consent management use-cases	**Link(s) to the UCS**
CREATE CONSENT AGREEMENT - Here, an organisation Administrator creates a Consent Agreement based on the Data Policy requirements.	UC-C-PIC-A-001
UPDATE CONSENT AGREEMENT - Here, an organisation Administrator updates the Consent Agreement based on the Data Policy requirements..	UC-C-PIC-A-002
READ CONSENT AGREEMENT - Here, an organisation Administrator reads the Consent Agreement.	UC-C-PIC-A-003
DELETE CONSENT AGREEMENT - a special case of consent agreement update	UC-C-PIC-A-004
CONSENT AGREEMENT CHANGE NOTIFICATION - Notifications for Data Providing and Data Consuming Systems, as well as Individuals upon changes to Agreement or Policy configuration.	UC-C-PIC-A-005

2.6.2 Individual User Functionalities

The table below summarises the key use cases identified for the Individuals.

Consent management use-cases	Link to the UCS
VIEW CONSENT - Here, the Individual views the Consent Agreement and the conditions for personal data processing (with adequate clarity for informed understanding). This includes obtaining copies of the consent agreement.	UC-C-PIC-I-001
GIVE CONSENT - Here, the Individual signs a Consent Agreement during a data sharing workflow. Note that this can also happen offline without data sharing in place.	UC-C-PIC-I-002
WITHDRAW CONSENT - Or update existing consent	UC-C-PIC-I-003
Consent agreement change notification	UC-C-PIC-I-004

2.6.3 Data Processing Auditor User Functionalities

The table below summarises the key use cases identified for the Data Processing Auditor.
Important note: In the Consent BB, we define the Data Processing Auditor's role (see 1.3 Terminology and 1.5.3 Actor definition) as an organisation's auditor implementing the Consent BB. The auditor role will most probably be akin to a Data Protection Officer (DPO), possibly from an external third party organisation and involve activities outside of the Consent BB.

To avoid ambiguity, we use the precise term Data Processing Auditor to stress the specificity of tasks to be performed by and for the Consent BB; all other actions not within the Consent BB's scope are considered as an external prerequisite and as a "black box" activity. With respect to audit, this role is distinguished from the data policy auditor.

Also to consider: "READ CONSENT STATUS" use-case is also used by any workflow (and Actor) that requires verification of the consent status (for example, before executing the data transfer from Data Providing System to Data Consuming System)

Consent management use-cases	Link to the UCS
AUDIT CONSENT - Query the Consents related to individuals or policies (opt-in/opt-opt)	UC-C-PIC-AT-001
MONITOR POLICY UPDATE- Tracking Data Policy changes and configuration conformance with it;	UC-C-PIC-AT-002
READ CONSENT STATUS - Viewing (reading, exporting) the Consent Agreements and relevant reports in a verifiable form	UC-C-PIC-AT-003
VERIFY CONSENT INTEGRITY - Ability to check the integrity of the signed agreements	UC-C-PIC-AT-004

2.7 Scenarios: Consent and Data Access

As described above under Universal Consenting Workflows, there may be an unlimited number of business processes that require consent. The following scenarios are but a few examples illuminating how appropriate access to data can and should be handled when processing or consuming data with the support of Consent BB functionalities.

Scenario	Source BB	Target BBs	Description
1.1 Querying: Which Consent Agreement is needed for specified data processing/ consumption?	Any	Workflow BB	Consent BB does have knowledge or state to resolve which Data Consumer or Data Producer requires consent. Everything regarding consent has a precondition that a decision is made and manifested in the Workflow BB or any other Data Consumer.
1.2 Data processing/ consuming system stores/fetches data with consent + prompts the user if none exists	Any	Consent BB	Given an Agreement ID and a User ID, the Consent BB can resolve if consent exists and possibly prompt the user. Workflow BB is especially inappropriate here because of UI integration and a blocking and sequential call stack.
1.3 Data processing/ consuming system stores/ fetches data with consent, no halts operations without consent	Any	Workflow	Given an Agreement ID and a User ID, the Workflow BB can complete an atomic action requiring consent. Operations shall not proceed if consent does not exist.
1.4 Data processing/ consuming system stores/ fetches data with consent, consent is prompted asynchronously	Any	Workflow	The Workflow BB may halt operations and asynchronously prompt the user for consent if none exists (or is invalid). After fetching consent, the Workflow BB should revert to the targeted data consuming/ processing operation.
1.5 Appropriate access to data that does not require consent	Any	Workflow	Not necessarily related to Consent BB
1.2-1.4 Side effects	Workflow		Any attempt to read consent and process/consume data is logged and auditable.

2.1 Inappropriate access: Data processing/ consuming system inappropriately stores/ fetches data without consent	Any	n/a	Any consent-requiring data access is assumed logged. Auditing of inappropriate data access is only possible when a log trace exists.
3.1	Workflow	Consent	Given an Individual, query if active Consent Records exist (for instance, to spot if other external data needs to be kept)
4.1	Any	Consent	Fundamental individual rights (GDPR / Data Protection Act etc): Right to be Forgotten
4.x	Any	Consent	Fundamental individual rights (GDPR / Data Protection Act etc): More TBD

3 Cross-Cutting Requirements

The Cross-cutting requirements described in this section are an extension of the cross-cutting requirements defined in the architecture specification document. This section will describe any additional cross-cutting requirements for this building block.

Cross-cutting requirements will use the same language (MUST or SHOULD) as specified in the architecture document.

Digital Registries BB	Must provide all functions related to the persistent storage of consent data.
Information Mediator BB	Shall provide functions to register Data Providers from which the Data Consumer will fetch the data.

3.1 Privacy

Personal data MUST be kept private and never shared with any parties, except where specific authorisation has been granted. The Consent BB shall follow the privacy principles as laid out in the Govstack architecture.

3.2Data Policy Audit Logging

Logs MUST be kept in a database of all created, updated, or deleted records. Logs MUST include timestamps and identify the user and affiliation that performed the transaction.

All audit logs shall be integrity protected against tampering. The Consent BB shall follow the data policy and audit logging requirements laid out in the Govstack architecture.

3.3Source Code and Licensing

A GovStack Building Block MUST be Open-source Only with No Vendor Lock-in.

3.4Security Requirements

In general, the Consent BB shall follow the security requirements as laid out in the Govstack architecture. Consent BB's API endpoints are invoked with a client-supplied API key which MUST defer to the Identification and Verification BB to verify the role and/or scope of the API key matches the API endpoint to which it is supplied. This is mentioned here as this Definition is drafted without clear guidance in the OpenAPI spec for handling roles and scopes.

MUST adhere to all requirements from Security BB requirements.

4 Functional Requirements

The functional requirements section lists the technical capabilities that this building block should have. These requirements should be sufficient to deliver all functionality listed in the Key Digital Functionalities section. These functional requirements do not define specific APIs - they provide a list of information about functionality that must be implemented within the building block. Subject-matter experts should define these requirements and don't have to be highly technical in this section.

4.1 Consent Agreement Configuration Requirements

Name	Description	Optionality
Create Consent Agreement	It shall be possible to create a consent agreement, either based on an existing or new data policy template. Each consent agreement shall be under version control.	MUST
View Consent Agreement	It shall be possible to view an existing consent agreement	MUST
Update Consent Agreement	It shall be possible to update an existing consent agreement.	MUST
Terminate Consent Agreement	It shall be possible to terminate an existing consent agreement	MUST
Revision history	It shall be possible to capture and sign all changes to Consent Agreements, Consent Policies and Consent Records in tamper-proof Revisions	MUST
Change notification subscription	It shall be possible to subscribe to enable or disable a change notification towards users	MUST

Name	Description	Optionality
Change notification	It shall be possible to trigger a change notification when there are changes done to an existing consent agreement	MAY
Logging	The BB shall log all administrative functions	MUST

4.2 Individual Consent Requirements

Name	Description	Optionality
View consent agreement	It shall be possible to view the associated consent agreement if it exists	MUST
Agree (Opt-in)	It shall be possible to agree or opt-in or sign a consent agreement	MUST
Withdraw (Opt-out)	It shall be possible to opt-out of a previously signed or agreed consent agreement	MUST
Logging	All individual consent actions shall be logged	MUST
Change notification subscription	It shall be possible to enable or disable consent change notification	MUST
Change notification	It shall be possible to trigger a consent agreement change notification towards individuals	MAY

4.3 Consent Audit Requirements

Name	Description	Optionality
Audit logging	All consent logs shall be tamperproof	MUST
View and verify the consent agreement	It shall be possible to view and verify a shared consent agreement	MUST
View and verify consents	It shall be possible to view and verify a signed consent agreement	MUST
Revision list	It shall be possible to filter and sort all objects' revision histories can be filtered and sorted	MUST

5 Data Structures

5.1 Resource Model

The resource model shows the relationship between data objects that are used by this Building Block. Data objects are ultimately modelled as OpenAPI schemas, however, as the relational model isn’t easy to understand from OpenAPI specification, we start by presenting two high-level Resource Models.

5.1.1 Simplified Resource Model

When an individual gives consent, it is implied that the Organisation from one side and the Individual from the other side digitally sign a Consent Agreement and a respective Consent Record is created. The alternative scenario may be that signing takes place offline on paper, but in this case, for Consent BB to function properly, it is the responsibility of the Organisation to digitise (eg scan) the signed document and create digitally signed artefact to represent the Consent Record,

This Consent Record is a digital instance referencing the Agreement which is consented to or subsequently has consent withdrawn from.

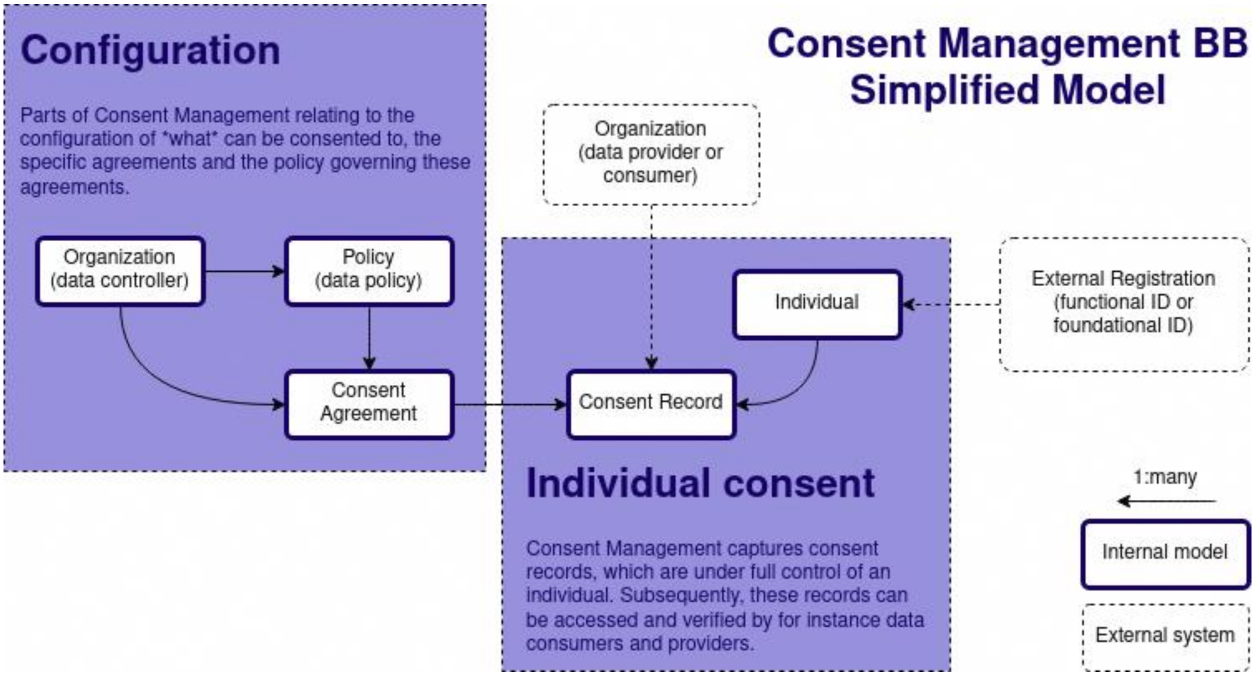
Configuration
Parts of Consent Management relating to the configuration of *what* can be consented to, the specific agreements and the policy governing these agreements.
Organization (data controller)
Policy (data policy)
Consent Agreement
Consent Management BB Simplified Model
Organization (data provider or consumer)
Individual
External Registration (functional ID or foundational ID)
Consent Record
Individual consent
Consent Management captures consent records, which are under full control of an individual. Subsequently, these records can be accessed and verified by for instance data consumers and providers.
1:many
Internal model
External system

Diagram Source

5.1.2 Elaborated Resource Model

This model expands the relationships between resources.

Revisions are maintained for Consent Records + Agreements and Data Policies, together with cryptographic signatures. This means that all changes are captured for auditability.

For a configured Agreement, data elements requiring consent are individually specified as Agreement Data.. Agreement Data is not directly relatable to processes and internals of an external system: This architectural choice gives the consent model flexibility and greatly simplifies the architecture and consent lifecycle, but it does not contradict any additional features, allowing for relations to external systems.

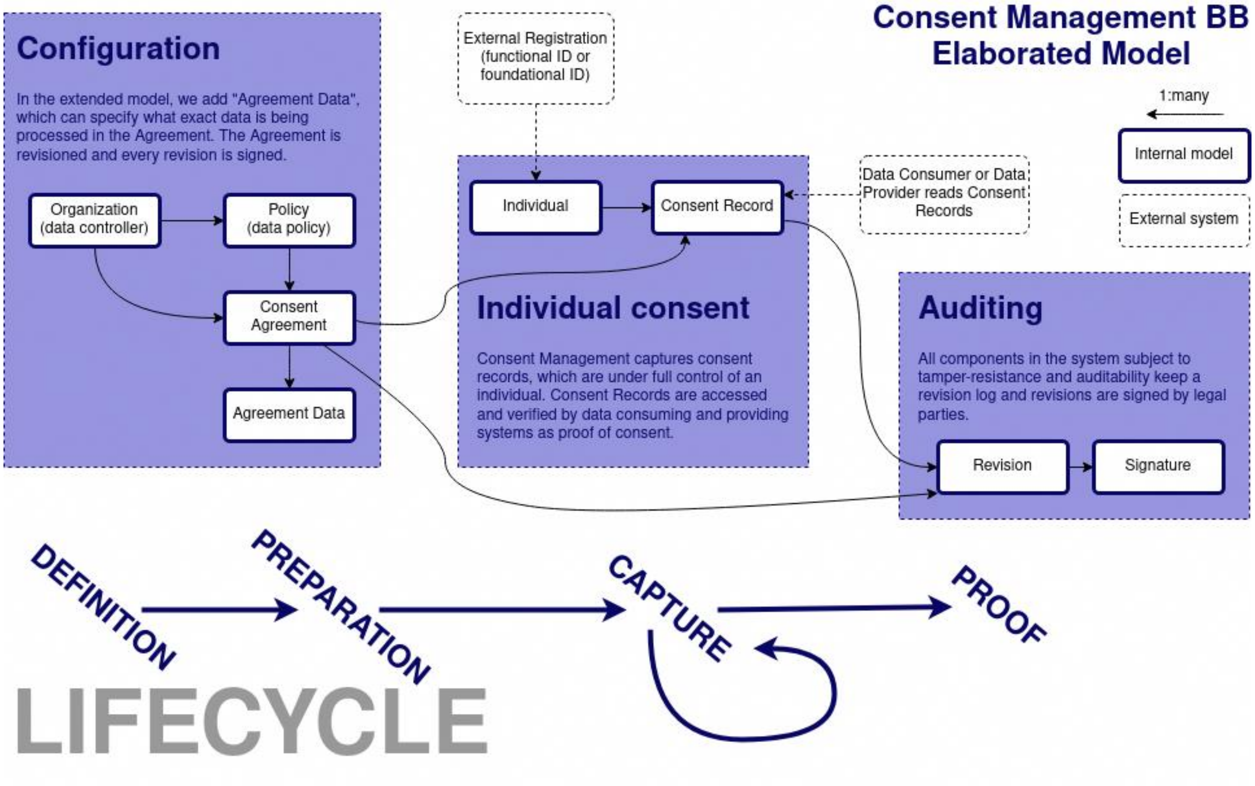
Consent Management BB
Elaborated Model
1:many
Internal model
External system
Configuration
In the extended model, we add "Agreement Data", which can specify what exact data is being processed in the Agreement. The Agreement is revisioned and every revision is signed.
Organization (data controller)
Policy (data policy)
Consent Agreement
Agreement Data
External Registration (functional ID or foundational ID)
Individual
Consent Record
Data Consumer or Data Provider reads Consent Records
Individual consent
Consent Management captures consent records, which are under full control of an individual. Consent Records are accessed and verified by data consuming and providing systems as proof of consent.
Auditing
All components in the system subject to tamper-resistance and auditability keep a revision log and revisions are signed by legal parties.
Revision
Signature
DEFINITION
PREPARATION
CAPTURE
PROOF
LIFECYCLE

Diagram Source

5.2 Use cases informing events

Generic:

- Individual changes Consent Record
- Individual withdraws/revokes Consent Agreement
- Consent Record expires
- Consent Record expiry date changes
- Organisation replaces Consent Agreement
- Organisation replaces Data Policy

Specific Use Cases:

- Individual gives access to citizen data, using a third-party UI (Consumer's UI). Example: COVID passports

5.3 Standards

The following standards are applicable to data structures in the registration building block:

- All dates should follow ISO 8601.

- RFC 7159 - The JavaScript Object Notation (JSON)
- OpenAPI Version 3.1.0
- RESTful APIs follow TM Forum Specification: "REST API Design Guidelines Part 1" (requirement derived from GovStack Architecture and Nonfunctional Requirements)

5.4 Data models

Data models are defined in Appendix A: Data models. This specification is seen as a minimum requirement, all further implementation may add more structure but should not compromise the minimal integrity laid out. All property types are generic, and a concrete implementation may add further specificity to these models.
The OpenAPI definition file is maintained in JSON format, and OpenAPI schemas may be interactively explored on Swagger Hub at Consent BB GitHub.

6 Service APIs

This section describes external APIs that must be implemented by the building block. Additional APIs may be implemented by the building block (all APIs must adhere to the standards and protocols defined), but the listed APIs define a minimal set that must be provided by any implementation.
A current API specification can be found here:

- API and Data model main definition document *(for commenting)*
- Pull-Request for 0.8 API spec *(raise PR if you want to suggest a change)*
- Latest version rendered API spec *(view only)*

Changes to the API definitions can be made by submitting a Pull Request on this repository.

7 Other Resources

Link to architecture requirements document (and specific sections within that document, such as cross-functional requirements, and general recommendations)

Link to use cases document – this document may be a valuable resource while developing workflows to ensure that a variety of different use cases are covered by the building block definition.

Link to BB criteria and maturity metrics document created by Tanvir

Link to Low Resource Settings document

Link to GitHub repository and OpenAPI documentation site for the building blocks.

8 Key Decision Log

Date	Decision
November-2021	Decided to scope and work on basic flows first with Consent BB version 1.0. This will scope out some items as described in chapter Out-of-scope and future enhancements
January-2022	Removed “consenter” and “consentee” terminology: Due to the ambiguity of what these two terms mean, we strictly mention only “individual”, “data processor” and “data controller”.
March-2022	The lifecycle of a single Agreement should match a single purpose. A Consent Record can only match 1 Agreement.
March-2022	Data structures, API URL call structures etc., should never reveal personally identifiable information (PII). We assume that anonymised IDs and tokens can handle relations to identity.
March-2022	Right To Be Forgotten: The scope of this action is decided to be framed by each Agreement. The building block definition covers a variety of different use cases deleted to remove traces or needs to be retained is not by design necessary for the Consent BB to decide.
March-2022	Revision+Signature models are designed to give a tamper-resistant, auditable track of all schemas. Auditability means: 1) Event-based external tracking that may verify that the system’s data isn’t tampered with and 2) Revision and Signature logs that can be queried to periodically verify that specific event (such as data transactions) is happening in accordance with valid Consent Records and Agreements.

9 Appendix A: Data Models

API model schema can be found in the latest API definition in either of these resources:

- https://docs.google.com/spreadsheets/d/1snIszqyTGYk1u25liwQ_1jONTsQeH7D8aqv1Td74xt4/edit#gid=1829058922 (**Note:** Please direct comments and suggestions to the working document)
- https://app.swaggerhub.com/apis/GovStack/consent-management-bb/ (interactive SwaggerHub OpenAPI rendition)
- https://github.com/GovStackWorkingGroup/BuildingBlockAPI/pull/15 (source YAML files)

Model	Description	Fields
Individual	Shallowly models an Individual which may reference some instance in an external system (registration system, functional ID, foundational ID etc). An Individual instance of this model is not to be mistaken with a unique natural individual. It is up to the system owner to decide if this record permits mapping to a natural individual and/or if a single Individual row can map to several consent agreements.	id, functional_id, foundational_id, session_id
Agreement	An agreement contains the specification of a single purpose that can be consented to. An Agreement is universal and can be consented to by *many* individuals through a ConsentRecord	id, version, controller, policy, purpose, lawful_basis, data_use, dpia, lifecycle, signature, active, forgettable
AgreementData	Agreement data contains specifications of exactly what is collected.	id, agreement, name, sensitivity, category, hash
Policy	A policy governs data and Agreement in the realm of an organisation that is referred to as \"data controller\" (GDPR) and owner of referencing Agreements.	id, name, version, url, jurisdiction, industry_sector, data_retention_period_days, geographic_restriction, storage_location
ConsentRecord	A Consent Record expresses consent (as defined in this building block's specification) to a single Agreement.	id, agreement, agreement_revision, individual, opt_in, state, signature

Model	Description	Fields
Revision	A *generic* revision model captures the serialised contents of any schema's single row. This is then subject to 1) cryptographic signature and 2) auditing. Aside from \"successor\" column, a revision should be considered locked.	id, schema, object_id, serialized_snapshot, timestamp, authorized_by_individual, authorized_by_other, successor, predecessor_hash, predecessor_signature
AgreementFilter	Query filter for API endpoint listing Agreement objects	id, name
ConsentRecordFilter	Query filter for API endpoint listing ConsentRecord objects	id, opt_in
PolicyFilter	Query filter for API endpoint listing Policy objects	id, name, revision
Controller	Details of a data controller.	id, name, url
Signature	A generic signature contains a cryptographic hash of some value, together with a signature created by some private key in another system. Required signing methods: Revision object or another Signature object.	id, verification_method, verification_hash, verification_signature, verification_artifact, jws_header, signed_by, timestamp, object_type, object_reference
AgreementPurpose	TBD: Models the purpose of an agreement	id, name, description
AgreementLifecycle	TBD: Models the valid lifecycle states of an Agreement	id, name
RegistryReference	TBD: When creating an Individual, we need some input that refers to a functional or foundational ID in an external system	id, foundational_id, functional_id

Model	Description	Fields
AuditTracker	TBD: An external tracker receiving information from the system that can be subject to external auditing and verification of correct behaviour. This is one of several notification/monitor/subscription patterns that may be more suitable for an encrypted Pub/Sub service.	id, name, public_key, callback_agreement, callback_consent_record, callback_policy, callback_revision_table_hash, callback_signature_table_hash
AuditEventType	TBD: Model for the possible events pertaining a change to an object subject to auditing. This model is not necessarily a database-backed model but part of application code.	id, event_name