# Data Protection & Privacy

This section describes how you can make your CAP application compliant with data protection and privacy requirements.

Table of Contents



## General Statement

Governments place legal requirements on industry to protect data and privacy.

> **TIP**
>
> No guide, including this one, concerning CAP attempts to give any advice on whether any features and functions are the best method to support company-, industry-, region-, or country-specific requirements. Furthermore, the information provided in this note does not give any advice or recommendations with regards to additional features that might be required in a particular environment. Decisions related to data protection must be made on a case-by-case basis, under consideration of the given system landscape and the applicable legal requirements.

For general information about data protection and privacy (DPP) on SAP BTP, see the SAP BTP documentation under Data Protection and Privacy .

# Data Protection & Privacy in CAP

CAP is a framework that provides modeling and runtime features to enable customers to build business applications on top. As a framework, in general, CAP doesn't store or manage any personal data on its own with some exceptions:

- Application logging on detailed level written by CAP runtime might contain personal data such as user names and IP addresses. The logs are mandatory to operate the system. Connect an adequate logging service to meet compliance requirements such as SAP Application Logging Service .
- A draft-enabled service `Foo` has an entity `Foo.DraftAdministrativeData` with fields `CreatedByUser` , `InProcessByUser` and `LastChangedByUser` containing personal data for all draft entity instances in edit mode.
- Messages temporarily written to transaction outbox might contain personal data. The entries are mandatory to operate the system. If necessary, applications can process these messages by standard CAP functionality (CDS model `@sap/cds/srv/outbox` ).
- Be aware that personal data might be added automatically when using the managed aspect.

Dependent on the business scenario, custom CDS models served by CAP runtime will most likely contain personal data that is also stored in a backing service.

CAP provides a rich set of tools to protect the application from unauthorized access to business data, including personal data. Furthermore, it helps applications to provide higher-level DPP-related functions such as data retrieval.

> **WARNING**
>
> **❗ Applications are responsible to implement compliance requirements with regards to data protection and privacy according to their specific use case.**

Also refer to related guides of most important platform services:

↳ *SAP Cloud Identity Services - Configuring Privacy Policies*

↳ *SAP HANA Cloud - Data Protection and Privacy*

## Data Protection & Privacy Supported by CAP

CAP provides several features to help applications meet DPP-requirements:

- The Personal Data Management (PDM) integration has a configurable **retrieval function**, which can be used to inform data subjects about personal data stored related to them.
- CAP also provides a *fully model-driven* approach to track **changes in personal data** or **read access to sensitive personal data** in the audit log. Having declared personal data in your model, CAP automatically triggers corresponding audit log events.

> **WARNING**
>
> ❗ So far, applications have to integrate SAP Data Retention Manager to implement an adequate **erasure function** for personal data out of retention period. CAP will cover an out-of-the-box integration in the future.