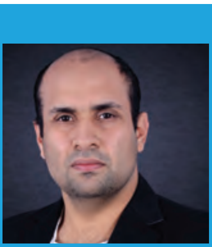
Support Regulatory Compliance Across Your SAP Landscape with SAP Data Privacy Integration

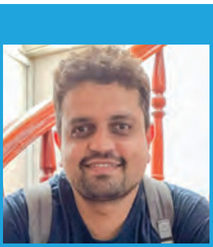
by **Prem Roshan Madhusudhan Nair** and **Sharath Jois**, Product Owners, Data Privacy Services, SAP

Digital data has continued to grow in volume over the years as organizations work toward modernizing their operations to take advantage of the various efficiency and innovation benefits of digital technologies. Of course, digitization and innovation bring new considerations as well. While companies are gaining access to more data than ever before — especially data about their customers — they are also facing new types of threats as hackers seek access to this valuable data, and new security requirements for landscapes that include the cloud. And with the COVID-19 pandemic driving a rapid increase in digital business as well as individuals' online activity, the protection of data — in particular, the protection of personal data — is front and center.

While it is important for businesses to ensure data privacy to gain the trust of both customers and business partners, the protection of this data is critical for adhering to the regulations that countries are introducing at a growing rate, with more data privacy bills introduced in 2020 compared to 2019. These regulations — such as the EU's General Data Protection Regulation (GDPR), the California Consumer Privacy Act (CCPA), and the Cybersecurity Law of the People's Republic of China — are designed to protect citizens by ensuring that their data is stored, processed, and deleted in a transparent and legally compliant manner.



PREM ROSHAN MADHUSUDHAN NAIR (prem.roshan.madhusudhan.nair@sap.com) has over 10 years of experience in SAP technologies. He has worked as a consultant for financial services solutions on the SAP NetWeaver platform, followed by developing business services on SAP Business Technology Platform. In his current role as a Product Owner for Data Privacy Services at SAP, he has worked on the development of requirements for data privacy use cases and data privacy solutions.



SHARATH JOIS (sharath.jois@sap.com) has over 10 years of experience in building and operating data privacy and data management tools on a wide range of platforms, including SAP NetWeaver ABAP, SAP Business Technology Platform, Cloud Foundry, and Kubernetes. As a Product Owner for Data Privacy Services at SAP, he has had the opportunity to drive the end-to-end life cycle of product development, from gathering requirements from customers, backlog ranking, and overseeing the end-to-end development cycle to commercializing, delivering, and marketing the product.

To comply with these types of regulations, businesses need to make sure that the applications they use to process personal data provide the required privacy protections. SAP offers SAP Data Privacy Integration for this purpose. This article explains how SAP Data Privacy Integration supports data privacy compliance in SAP customer landscapes. It first explains important data privacy concepts, and then walks through the data privacy and integration features the service provides to support compliance across multiple applications throughout the enterprise.

Key Data Privacy Concepts

Before diving into how SAP Data Privacy Integration can help organizations fulfill their data privacy obligations, it will help to understand some key data privacy concepts, such as what is considered personal data, the roles involved in the processing of personal data, when businesses can process personal data, and the rights of data subjects when it comes to their personal data. Note that while each specific regulation has its own terminology for data privacy concepts, the following sections follow the terminology established by GDPR, which SAP uses in most data privacy discussions.

What Is Personal Data?

Personal data is any information — such as address, telephone number, and IP addresses — that can be used to directly or indirectly identify a living person (see **Figure 1**).

Attributes that can be used for direct identification — that is, information that can be used alone to identify someone — include:

- Name
- Address
- Telephone number
- Email address

Information that can be used for indirect identification — that is, information that can be used to identify someone only in combination with other information — includes:

- IP address
- MAC address
- License plate number
- Insurance number

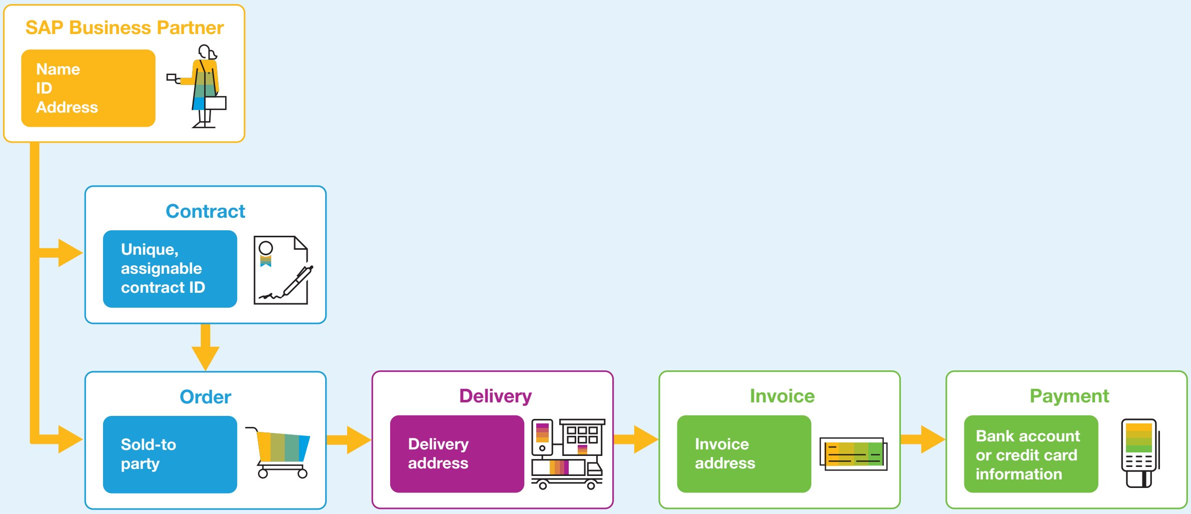


Figure 1 Personal data is any information — such as address, telephone number, and IP addresses — that can be used to directly or indirectly identify a living person

What Roles Are Involved in Processing Personal Data?

It is also important to understand the three key roles that are involved in the processing of personal data:

- The **data subject** is the user or person whose personal data is being stored or processed. An example is an employee of an organization.
- The **data controller** is a person or legal entity responsible for the lawful processing of personal data for the data subject. An example is an employer that signs a contract with an employee to process personal data.
- The **data processor** is a person or legal entity that processes personal data on behalf of and in accordance with the instructions of a data controller. An example is a cloud-based human resources application provider that processes the personal data of a data subject according to the instructions of an employer.

When Can Personal Data Be Processed?

Organizations must have a valid business purpose or legal basis for processing someone's personal data. A valid business purpose is defined as:

- Execution of a contract
- Freely given consent
- Fulfillment of a legal obligation
- Vital interests of a data subject
- Overriding legitimate interest

More information on valid reasons for processing personal data can be found in Article 6 of the GDPR.

What Are the Rights of Data Subjects?

Data privacy regulations across the globe provide basic rights for data subjects when it comes to how data controllers and data processors handle their data. These rights include:

- **Right to information**: The data subject has the right to know if any personal data is being processed by the data controller, including the purposes for which that data is being processed and the categories of the data being processed (contact information or payment information, for example). A copy of the personal data must also be provided to the data subject upon request.
- **Right to be forgotten**: The data subject must have an option to trigger the deletion of personal data when the data controller no longer needs it to fulfill the business purpose for which the data was collected. The data should be marked for deletion upon the withdrawal of the data subject's consent or any other legal basis for the processing of that data.
- **Right to export data**: The data subject can request an export of the personal data processed by a data controller in a machine-readable format to enable easy movement of the data from one controller to another — to switch service providers, for example — as required by Article 20 of the GDPR.

A Cloud Service for Data Privacy Across End-to-End Processes

To comply with data privacy regulations, the applications an organization uses to process personal data must have the capabilities necessary to support the rights of the data subject. In smaller, simpler landscapes, where a business process or use case is performed within a single application (where all sales functions are managed by one sales solution, for example), simple data deletion and reporting capabilities can provide this compliance. In larger enterprise business landscapes, where complex business processes are performed by multiple applications running on different technology stacks, adhering to data privacy requirements becomes increasingly complex.

For example, in SAP landscapes, the total workforce management or hire-to-retire business process begins with employee onboarding in an SAP SuccessFactors system, for instance, and the distribution of the employee master data to multiple systems, such as SAP S/4HANA and SAP Concur. In these types of scenarios, as part of fulfilling an employee contract, the data subject — in this case, the employee — may use a front-end system to provide personal data that is then transferred or replicated across the different systems in the landscape. The business context or reason for processing the data can then get lost in downstream systems, which can make it difficult to identify the business purpose for processing the data and report or delete it at the end of its purpose.

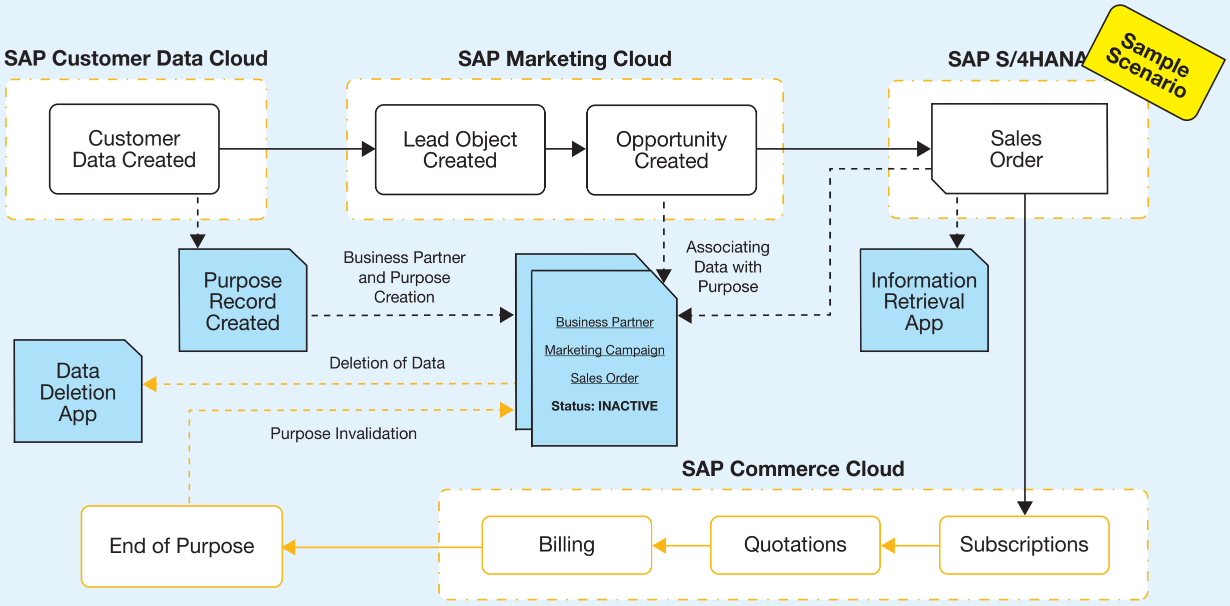


Figure 2 Purpose-based processing of personal data in an example end-to-end business process

SAP Data Privacy Integration is a service available on SAP Business Technology Platform (SAP BTP) that provides capabilities for managing the privacy of personal data in end-to-end business processes, including those enabled by SAP's Intelligent Suite or any other applications that integrate with the service. Its features can help organizations fulfill data privacy requests and adhere to data privacy regulations, and include centralized configuration and management of business purposes, information reporting and retrieval, and data deletion functionality. We'll look at each of these areas in turn next.

Business Purpose Management

To support end-to-end data privacy, SAP Data Privacy Integration provides functionality for the centralized configuration and management of the business purpose for data. The defined business purpose brings together the legal basis for processing the personal data of the data subject, the data controller responsible for processing that personal data, the business processes that can be executed using that personal data, and the categories of the personal data that can be processed based on this purpose.

When a data subject is part of a business process in which personal data is collected for a purpose, SAP Data Privacy Integration can use application programming interfaces (APIs) to create a central instance of the business purpose for that data. Any applications across the landscape that store that data can reference that central instance of the business purpose.

Figure 2 shows an example scenario. As you can see, in a typical sales scenario, there can be multiple IT systems processing customer data. There could be a marketing system using the customer's personal data for promotional purposes as well as an ERP and commerce solution for stock-keeping and billing purposes, which would also process the customer's personal data. In this type of scenario, the contract signing during customer onboarding can be used as the event for creating a purpose record for the customer. This central purpose record is then referenced by the different applications in the landscape to process the customer's personal data.

With a central instance of the business purpose within SAP Data Privacy Integration, it becomes easy to discover personal data stored across the different applications in the landscape, and when the purpose

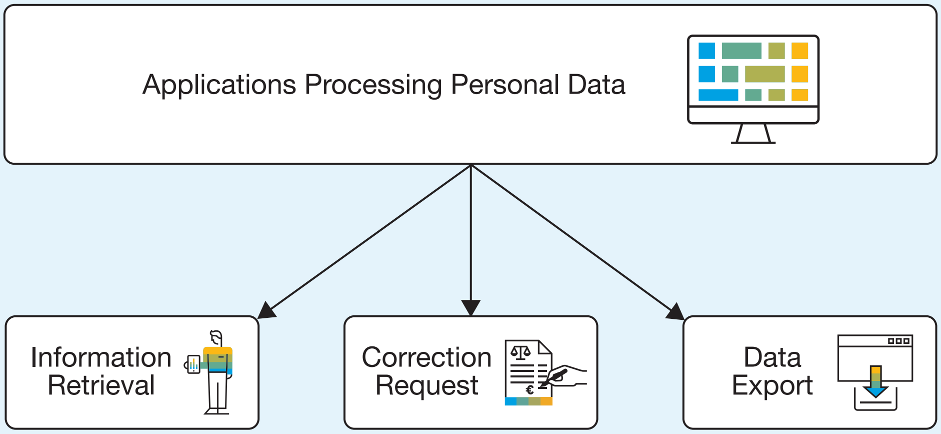


Figure 3 Information reporting and retrieval is one of the most common data privacy requests

is no longer relevant, such as when a contract has expired or consent is no longer relevant, it becomes easier to trigger the retention or deletion of the data as necessary.

Information Reporting and Retrieval

Information reporting and retrieval, which addresses the data subject's right to information and right to export data, is one of the most common data privacy requests (**Figure 3**). In this case, data subjects request information about their personal data stored in the organization's systems. This request is usually made to determine if any data is being processed by the data controller without the knowledge of the data subject or is being processed beyond the defined business purpose.

In addition, data subjects can request changes or corrections to any of their personal data that is stored by the organization, such as a change of address, and can request that their data be exported in a machine-readable format so that it can be easily imported into a new target landscape. For example, the data subject may want to transfer the data to another vendor or service provider, or from one hyperscaler to another.

SAP Data Privacy Integration also enables customer service representatives to perform these tasks on their own, without the need to involve IT. Using the provided features, they can discover the personal data of a data subject, trigger the export of that data, and send that data to the data subject as an email message or as a file (a PDF, JSON, or XML file, for example).

Data Deletion

Along with ensuring that personal data is processed only for a valid purpose and that only the data agreed upon by the data subject is processed, it is crucial to ensure that personal data is removed from the system when there is no longer a business need for it. This is also referred to as the right to be forgotten or the right to delete personal data from the system.

It is important to keep in mind that although data subjects have the right to delete personal data, enterprise systems require that data for a certain period of time to ensure that business needs can be met, such as order delivery or audit requirements. This means that data cannot necessarily be deleted immediately upon request. What is required for compliance is that the data be deleted when there is no longer a business need to process the data.

Within SAP Data Privacy Integration, this compliance can be realized by configuring deletion periods for the required data set. These deletion periods are defined as the residence period and the retention

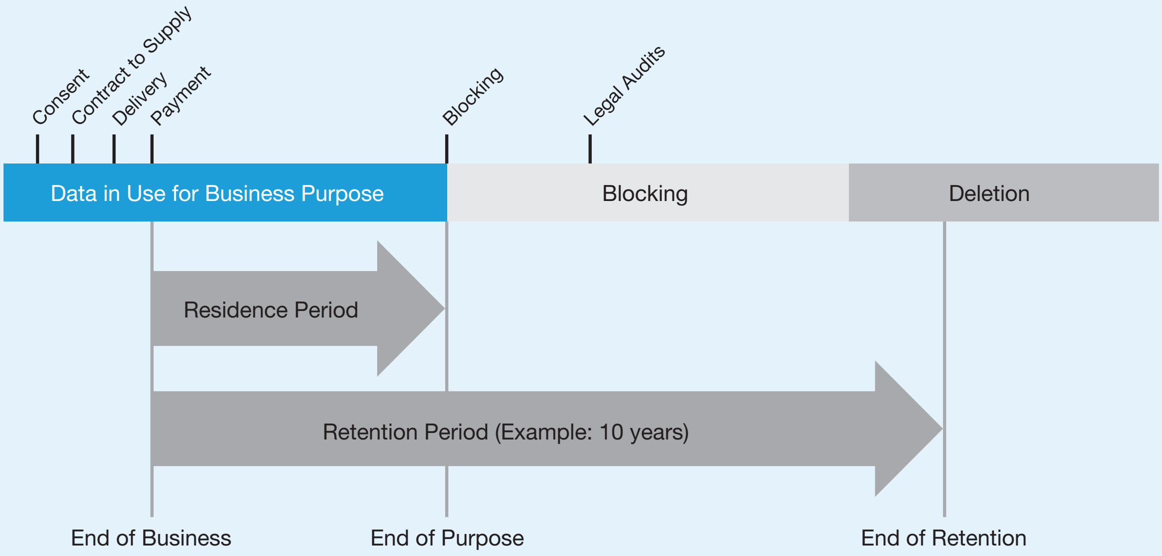


Figure 4 SAP Data Privacy Integration helps meet data deletion requirements with configurable deletion periods

period (see **Figure 4**). The residence period is the period of time after the end of the business purpose, when there is no need to store contact details for marketing purposes, for instance. During this period, the data can be anonymized or stored in secondary persistence in the system, rather than in primary persistence, to ensure that it is no longer processed (to receive marketing emails, for example). The data then remains in an inactive state to fulfill audit requirements, for instance, during what is called the retention period. At the end of the retention period, the data can be permanently deleted from the system (see **Figure 5**).

SAP Data Privacy Integration provides features for configuring rules for these periods of time and orchestrates the deletion of data by performing an end-of-purpose check for the data across the different applications integrated with the service. When the end-of-residence or end-of-retention period is reached, the service provides the necessary trigger to block or delete the personal data.

Integrating Applications with SAP Data Privacy Integration

A license to SAP Data Privacy Integration can be purchased as part of an SAP customer's Cloud Platform Enterprise Agreement or via SAP Store, after which the service can integrate with applications. **Figure 6** provides a high-level overview of the steps required to integrate applications with SAP Data Privacy Integration.

Once the service is added to the customer's global account, an instance of the service must be created that includes the configuration required to integrate with applications containing personal data. The configuration specifies the data objects and entities that contain personal data as well as the interfaces through which data can be accessed to realize the data privacy use cases. More in-depth information about these steps is available in the online SAP Help Portal.

Let's take a closer look at the interfaces and runtimes that support the integration between the service and business applications.

Supported Interfaces

SAP Data Privacy Integration does not store or persist any personal data processed by a business application. The service can report, manage business purposes, or delete personal data by interacting with an application using well-defined interface technologies, such as the Representational State Transfer (REST) and Open

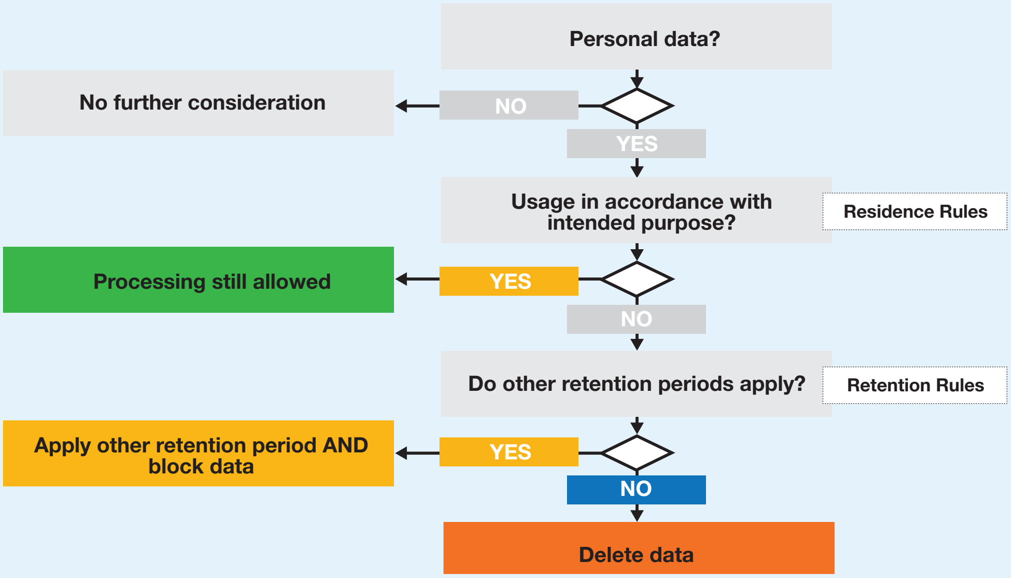

Personal data?
No further consideration
NO
YES
Usage in accordance with intended purpose?
Residence Rules
Processing still allowed
YES
NO
Do other retention periods apply?
Retention Rules
Apply other retention period AND block data
YES
NO
Delete data

Figure 5 SAP Data Privacy Integration provides features for defining the life cycle of personal data in the system

Data (OData) protocols, to read data for reporting purposes and trigger deletion of data. Annotations in the data model of business applications identify the business objects and entities that are relevant to data privacy or contain personal data.

Annotations in the data model also help categorize the personal data in an application, such as contact data, address data, and payment details. In addition, annotations can be used to differentiate personal data from sensitive data, which is anonymized for all scenarios except when the data is provided directly to the data subject.

More information on the interfaces supported by SAP Data Privacy Integration can be found at SAP API Business Hub.

Supported Runtimes

SAP Data Privacy Integration is available as a service for applications that process personal data and can integrate with SAP BTP technologies. To integrate an application with SAP Data Privacy Integration, an instance of the service must be created within the runtime environment of the business application — the runtime environment is Cloud Foundry in the

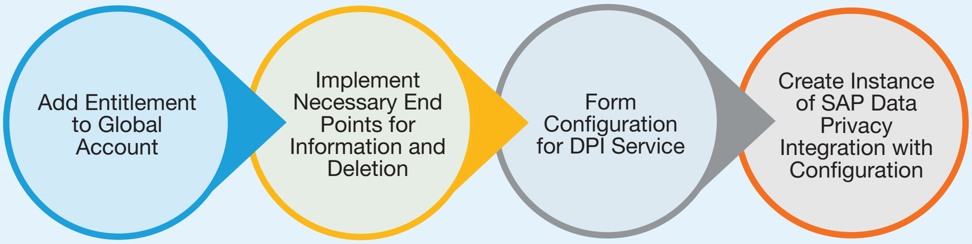

Add Entitlement to Global Account
Implement Necessary End Points for Information and Deletion
Form Configuration for DPI Service
Create Instance of SAP Data Privacy Integration with Configuration

Figure 6 A high-level overview of the steps required to integrate applications with SAP Data Privacy Integration

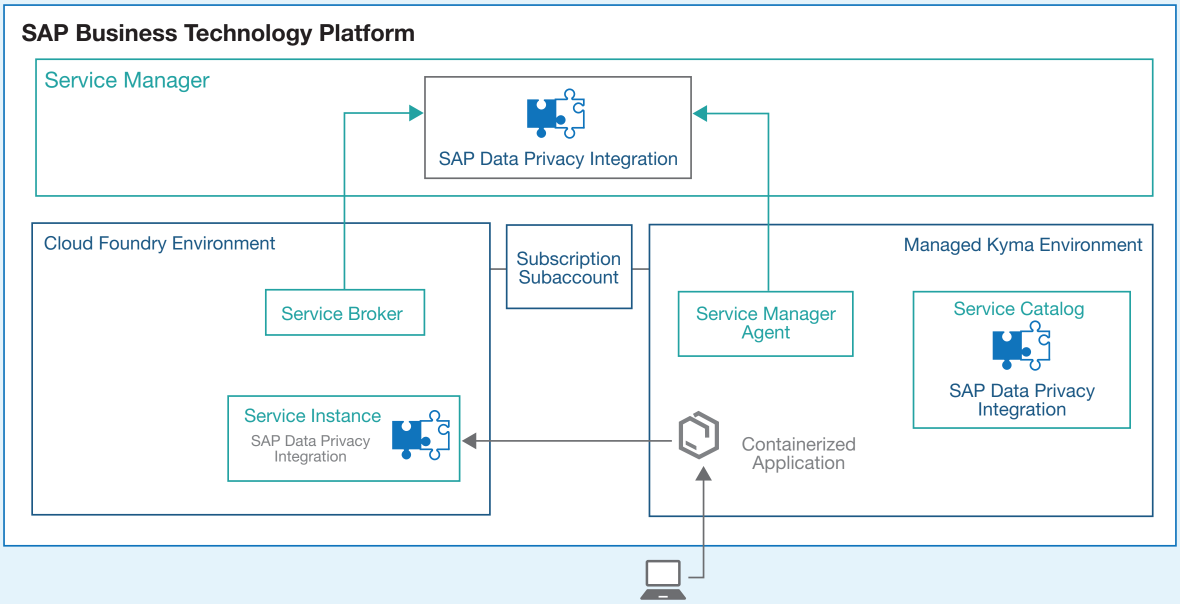

SAP Business Technology Platform
Service Manager
SAP Data Privacy Integration
Cloud Foundry Environment
Subscription Subaccount
Managed Kyma Environment
Service Broker
Service Manager Agent
Service Catalog
SAP Data Privacy Integration
Service Instance
SAP Data Privacy Integration
Containerized Application

Figure 7 To integrate an application with SAP Data Privacy Integration, an instance of the service must be created within the runtime environment of the business application

example shown in **Figure 7**. The instance is created using a service broker based on the Open Service Broker API (OSBAPI) specification.

The service broker is registered with the service manager component of SAP BTP, which allows the service to be instantiated from any landscape that provides a service catalog based on the service manager implementation. These landscapes include the Cloud Foundry and Kubernetes (Kyma) runtimes provided by SAP, and can be extended to any landscape that can create a service instance using the service manager client.

Details on how applications in different runtimes can integrate with SAP Data Privacy Integration are available in SAP Help Portal.

LEARN MORE

- **SAP Discovery Center**

  https://discovery-center.cloud.sap/#/serviceCatalog/data-privacy-integration
- **SAP Help Portal**

  https://help.sap.com/viewer/product/DATA_PRIVACY_INTEGRATION/SHIP/en-US
- **Data Privacy Integration overview video**

  https://youtu.be/tms6_AEy2q8

Conclusion

SAP Data Privacy Integration became generally available in Q3 2020. SAP customers and partners that build applications on SAP BTP using either Cloud Foundry or Kyma as their runtime can consume SAP Data Privacy Integration as part of their Cloud Platform Enterprise Agreement or by purchasing the license from SAP Store. The service is also available for partner testing scenarios in the SAP PartnerEdge portal through the partner test, demo, and development license.

SAP customers and partners that build applications on SAP BTP can look to SAP Data Privacy Integration as a starting point for fulfilling the requirements of data privacy regulations. With SAP Data Privacy Integration providing data privacy features, organizations can focus on using their business applications to power their digital transformation journey. ■