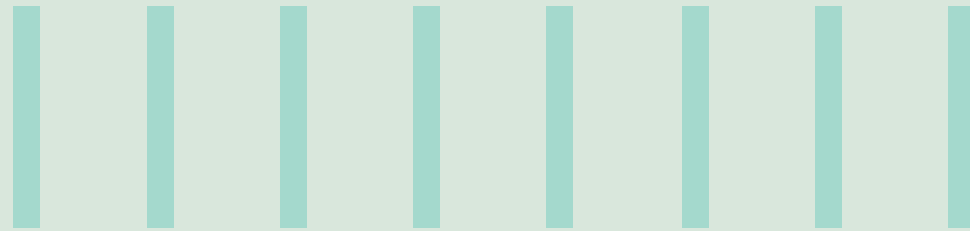




NAVIGATING DATA RESIDENCY REGULATIONS: SAFEGUARDING PII DATA THE RIGHT WAY

CRM SOLUTION IN THE ABSENCE OF HYPERFORCE IAAS



Abstract

With increasingly stringent industry and country-specific regulations on personally identifiable information (PII) coming into place, addressing data residency regulations is critical for businesses using Salesforce. This white paper investigates strategies to design effective solutions within the Salesforce ecosystem, ensuring compliance for core CRM and marketing cloud operations. It outlines integration patterns, such as Salesforce Connect and middleware, to keep PII data on-premises while fully leveraging Salesforce's capabilities. The paper also addresses the limitations and challenges of these approaches, recommending a shift to Salesforce Hyperforce for improved scalability, security, and compliance. Adopting Hyperforce is crucial for regulatory compliance and enhancing overall system performance.

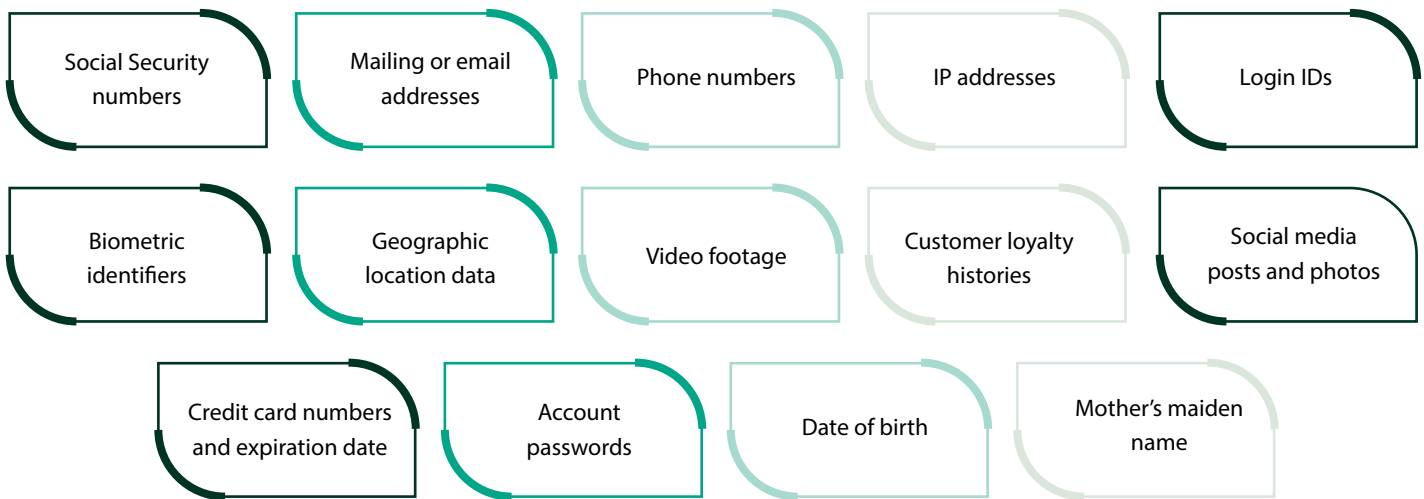
Introduction

Most countries do not allow local customer personally identifiable information (PII) data to be stored outside the country in line with industry-specific and country-specific regulatory requirements. While the Salesforce platform is globally accessible, servers utilized for Salesforce Hyperforce hosting application and operation data can only be accessed in a limited number of countries. These are the US, Japan, Germany, the UK, and France. As Salesforce Hyperforce continues to expand to include more server hosting countries, it ensures that PII data is stored locally on country premises, while the rest of the CRM data can be stored on SaaS platforms outside the country.

This paper discusses the approach to achieving a viable solution design and/or architecture pattern to address data residency challenges in Salesforce's core CRM and marketing cloud. It also covers some of the limitations associated with this type of design pattern.

List of PII Fields

Personally identifiable information is defined by different regulatory bodies as data, whether or not true, about an individual that can be (a) derived from the data; or (b) derived from the data and information to which an organization may have access. While this list is not exhaustive, it includes:



How Companies Can Overcome Data Residency Regulatory Challenges in Salesforce

Keeping PII Data Outside Salesforce

To store data on-premises, there is a need for a middleware or Salesforce connector for the on-premises database to interface with the Salesforce platform.

Fetching the details into Salesforce is done via:

1. Salesforce Connect
2. MuleSoft (middleware)

The customer needs to have a local on-premises data source (some kind of master data management or MDM for leads, contact, party, individual, address, and other personally identifiable information). It is assumed that the customer uses Azure data table services, Microsoft SQL servers, or a Mongo DB for this purpose.

Salesforce uses Salesforce Connect (previously known as Lightning Connect) where a custom external object created and mapped into Salesforce works with Salesforce Connect to fetch, update, or create the data records from or into the MDM (on-premises data source).

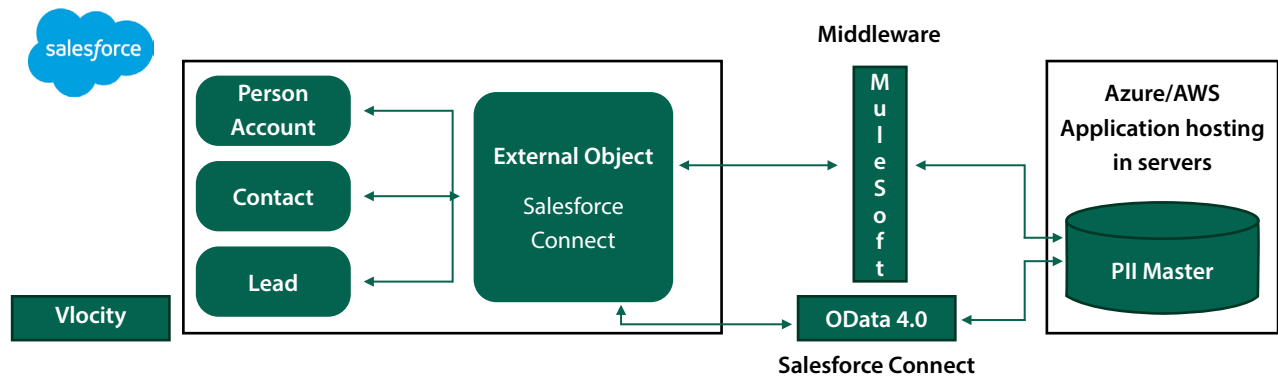


Fig 1: Simple conceptual depiction of Salesforce Connect.

Salesforce Connect supports the following integration patterns:

Connect to other APIs:

This approach utilizes the Apex connector framework (customization) to connect, fetch, and update records. It is used for non-OData protocol supporting data source systems. Here, external objects are used from a Salesforce perspective; however, external objects would fetch PII details in real-time from the data source using an Apex adaptor.

Connect via middleware:

This involves integration through middleware solutions such as MuleSoft, Apigee, or Fusion within a customer context. This method is suitable for write operations.

Connect to Salesforce:

Leveraged for multiple instances of Salesforce, this easy-to-use adapter can link external applications without requiring coding.

Connect via OData APIs (OData v4.0):

Ideal for point-to-point integrations where enterprise middleware is unavailable. This requires external systems that expose OData-compliant endpoints and is suitable for both read or write operations.

Writable external objects:

This lets the Lightning platform and users in the organization create, update, and delete records for external objects associated with the external data source. The external object data is stored outside the organization and external objects are read-only by default.

- Create external data sources
- Create external objects and fields
- Create relationships between data objects in the external source and your Salesforce instance

Other Considerations While Using the Salesforce Connect Option

Salesforce Connect's global search option can be utilized for search on the data store.

An external ID with Salesforce and data source is encrypted and used to link up the data.

One should avoid logging the information within Salesforce, such as custom trace/log objects.

Building reports within Salesforce leveraging external object records may reach governance limits and impair performance.

Due to the lack of customer key details within the core CRM, implementing customer-centric features around Einstein capabilities, email-to-lead, email-to-case and live person chat or messaging, including social CRM features, become more challenging.

The PII details on external objects cannot have validation rules, formulas, triggers, workflows, or process builders applied to them.

Dealing with PII Files or Attachments

1. PII data-generated documents should be stored in the on-premises data store. The hyperlink can be stored in Salesforce and opened by clicking on it. The document can be in an encrypted format. While clicking on the hyperlink, the document is decrypted in the on-premises data store and then opened. (The encryption part is optional since the documents are only stored on-premises.)
 - a. It is possible to use the customer's Azure or DocHub, or even a local file storage solution.
2. There are maintainability cost impacts on functionality extension with on-premises document storage. There is also the risk of data integrity issues based on source system changes.

In addition to storing PII data externally and fetching it via Salesforce Connect on demand, if there are any unavoidable PII fields that need to be stored locally within Salesforce, and if one or two PII fields do not identify a person, then Shield encryption can be an option. With Salesforce Shield, one can securely encrypt Salesforce data at the field level with AES-256-bit encryption and manage encryption keys on the platform.



Key Insights from Platform Encryption

AES 256-bit encryption:

This is the highest level of encryption available within Salesforce.

At-rest encryption:

It encrypts the data “at rest”, that is, when the data is not being processed in the data center. The data is stored as ‘cipher text’ (it converts plain text into a cipher text). As a result, the real data is not readable by database agents working at Salesforce database centers.

Manage your own encryption keys:

There are three ways to manage encryption keys in Salesforce. Encryption keys can be generated in Salesforce. However, customers with an existing key management infrastructure will benefit from the “bring your own key” (BYOK) approach.



Encrypt data at the field level:

Field-level encryption is not built into Salesforce.

Encryption policy:

This policy encrypts files and attachments in an “all or nothing” manner (i.e., not selectively according to certain files).



Encryption scheme for customer data (probabilistic or deterministic), depends on use cases and field data types and purposes. The trade-offs are available here: https://help.salesforce.com/articleView?id=security_pe_deterministic_considerations.htm&type=5

Process Flow

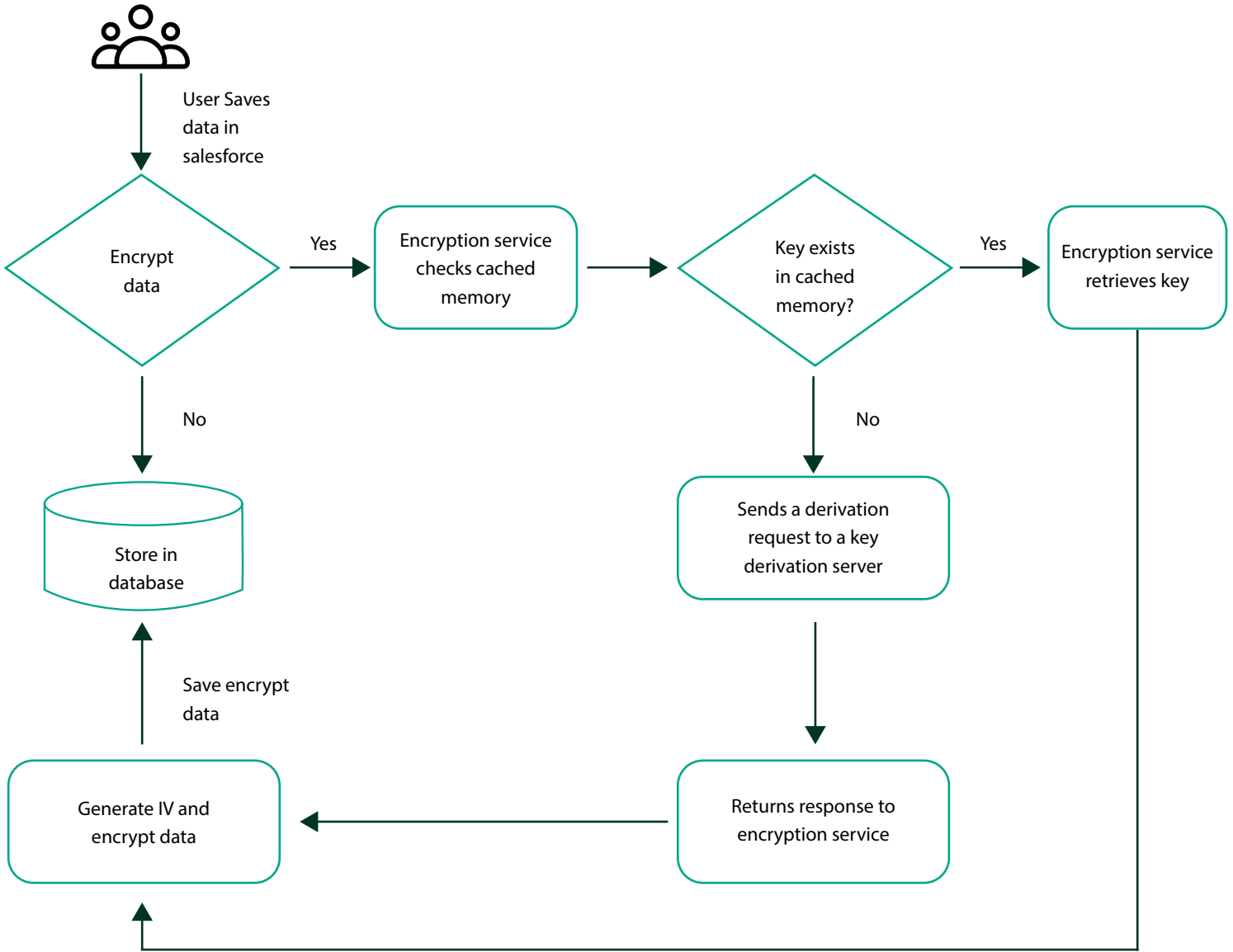


Fig 2: Salesforce Shield Platform Encryption





Considerations to Move Away from External PII Data Management

It is wise to take advantage of this opportunity by collaborating with Salesforce's success community. By having a locally hosted Hyperforce PaaS/IaaS instance and moving externally stored PII data into the core CRM platform, one can repoint all the middleware for read/write from the core CRM and gradually retire any externally stored PII database that was created as a stand-alone solution. This helps the core CRM platform scale and bring new features to your client's CRM IT ecosystem.



Salesforce Hyperforce delivers:

Data Residency:
Hyperforce lets customers serve their employees and customers globally while providing choice and control for residency and compliance.




Scalability:
Customers can grow and scale their business more flexibly and sustainably.

Security:
Hyperforce is secure by default, with least-privileged control, zero-trust principles, and encryption of customer data at rest and in transit.



Privacy:
Hyperforce provides comprehensive privacy standards that give clients control and transparency over their customers' data.

Agility:
Hyperforce increases agility with no downtime for releases and general maintenance, faster development and test environments, and extensive interoperability with AWS. Downtime may be required during organizational migrations or major technology upgrades.



Conclusion

The Hyperforce IaaS solution offers scalability, elasticity, and compliance with the data residency requirements of various countries and industries. In the absence of a Hyperforce setup as an alternative, storing PII details externally and fetching them via Salesforce Connect with Shield-based encryption ensures regulatory compliance and the ability to perform core transactions. The solution described above does come with various use-case limitations which must be discussed, documented, and addressed based on stakeholder alignment. The external storage of PII details must be seen as a tactical placeholder solution and not as a strategic one. It is advisable to move to Hyperforce IaaS at the earliest opportunity to unlock various CRM use cases and productivity improvements.

About the Authors



Gunjan Patel

Gunjan Patel has nearly fifteen years of experience in CRM application architecture and platform advisory services for cloud-based applications. He has been part of numerous digital transformation journeys for various industry verticals and specializes in Telecom B/OSS space.



Dr. Thejasvi Nagaraju

Dr. Thejasvi Nagaraju has nearly twenty years of experience in domain consulting and platform advisory services for cloud-based enterprise applications. He is closely associated with Salesforce based digital transformation journeys and specializes in Telecom B/OSS space.

Infosys Cobalt is a set of services, solutions and platforms for enterprises to accelerate their cloud journey. It offers over 35,000 cloud assets, over 300 industry cloud solution blueprints and a thriving community of cloud business and technology practitioners to drive increased business value. With Infosys Cobalt, regulatory and security compliance, along with technical and financial governance come baked into every solution delivered.

For more information, contact askus@infosys.com

Infosys[®]
Navigate your next

© 2024 Infosys Limited, Bengaluru, India. All Rights Reserved. Infosys believes the information in this document is accurate as of its publication date; such information is subject to change without notice. Infosys acknowledges the proprietary rights of other companies to the trademarks, product names and such other intellectual property rights mentioned in this document. Except as expressly permitted, neither this documentation nor any part of it may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, printing, photocopying, recording or otherwise, without the prior permission of Infosys Limited and/ or any named intellectual property rights holders under this document.

[Infosys.com](https://www.infosys.com) | NYSE: INFY

Stay Connected   