

SAP Solution Brief

Solution Extensions | SAP Data Encryption by CipherCloud

Advanced Protection of Employee Data in SAP® SuccessFactors® Solutions





Meet strict privacy and data protection requirements

Many companies employ SAP® SuccessFactors® solutions to dramatically improve their human capital management (HCM) practices and secure their employee data in the cloud. But organizations in heavily regulated industries often need to go further to comply with privacy and data residency requirements and **protect employee data** – especially when transmitting data through the cloud.

Meet strict privacy and data protection requirements

Safeguarding personal data is a critical priority. But organizations in certain sectors – such as federal governments, public sector, and financial services – must comply with more stringent data protection regulations. Even where these strict regulations may not apply, many data privacy officers, legal departments, and chief information security officers are mandating that organizations deploy advanced data protection technologies for their HCM systems and demonstrate that the organization has absolute control over personal data.

However, this protection must not adversely impact business functionality, such as the ability to search on or filter encrypted data, perform analytics, or produce e-mail notifications. The right solution should also support integration of HCM applications with other back-office software.

The SAP Data Encryption solution by CipherCloud provides comprehensive encryption features that help companies meet data protection, privacy, and residency mandates.



Boost security with advanced data protection

SAP Data Encryption offers powerful features to help organizations with strict data protection requirements use SAP SuccessFactors cloud solutions. It provides advanced data protection by deploying an in-line gateway that acts as a centralized control point, applying encryption and tokenization to sensitive data as it moves to the cloud.

The solution encrypts personally identifiable information (PII) elements in SAP SuccessFactors solutions whether data is in transit, at rest, or in use. Encryption in use lets you take action on encrypted data without first decrypting it outside the network. Organizations can put sensitive, confidential, and regulated data into the cloud while retaining direct ownership and control (see the [figure](#) on the next page).

Boost security with advanced data protection

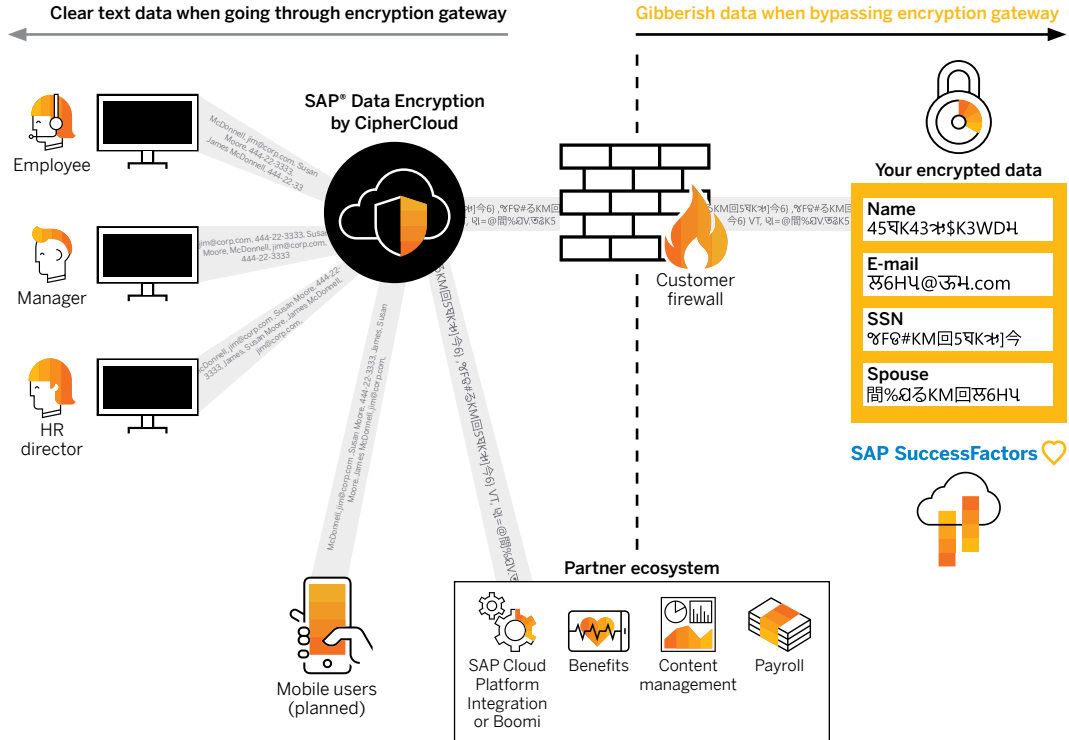
Preserve critical functionality for protected data

Integrate with other business software

[Continued on page 5](#) >>



SAP Data Encryption lets you take advantage of advanced cloud applications while helping to ensure privacy and compliance.



Boost security with advanced data protection

Preserve critical functionality for protected data

Integrate with other business software

Protecting data using SAP Data Encryption by CipherCloud



Zero-knowledge key management helps you maintain full control of encryption keys. With SAP Data Encryption, you own the encryption keys. SAP SuccessFactors solutions can never decrypt your encrypted data or pass it on to other cloud service providers, thus preventing unauthorized access or forced legal disclosure without your knowledge.

Using Advanced Encryption Standard (AES) 256-bit encryption, the solution preserves the format and searchability of protected data. It also supports key storage on Key Management Interoperability Protocol (KMIP)-compliant servers.

SAP Data Encryption also helps you adhere to industry security standards and certifications, such as the European Union General Data Protection Regulation (GDPR) and National Institute of Standards and Technology (NIST) standards. The CipherCloud encryption appliance used for



Get the power you need to meet strict privacy and residency laws for employee data with SAP Data Encryption.

SAP Data Encryption has achieved Federal Information Processing Standard (FIPS) 140-2 level 1 validation, a U.S. government computer security standard. You can also achieve FIPS 140-2 level 2 and level 3 validations with additional configuration.

Boost security with advanced data protection

Preserve critical functionality for protected data

Integrate with other business software



Preserve **critical functionality** for protected data

SAP Data Encryption provides excellent data protection without sacrificing key business functionality in your SAP SuccessFactors solutions, such as reports, searches, sorts, or e-mail notifications.

For ad hoc reporting and workforce analytics, the solution preserves features such as organizational charts, filters, and online views. It also protects data in downloaded and scheduled reports. For e-mail notifications, SAP Data Encryption safeguards e-mail addresses, subject lines, body text, and attachments by encrypting them.

Protected fields include personal and sensitive data such as employee name, address, e-mail address, national identification numbers, emergency contacts, and sensitive pick list data. The solution also preserves user interactions with protected data, including inputs, views, searches, sorts, and organization charts.



Protect employee data while maintaining the functionality in your SAP SuccessFactors software for HCM? With SAP Data Encryption, you can do both.

Boost security with advanced data protection

Preserve critical functionality for protected data

Integrate with other business software



Integrate with other business software

SAP Data Encryption is based on an open platform that allows you to integrate with your complete HCM ecosystem while keeping your employee data secure. In the SAP SuccessFactors solution family, SAP Data Encryption works with SAP SuccessFactors Employee Central, SAP SuccessFactors Learning, SAP SuccessFactors Performance & Goals, SAP SuccessFactors Compensation, and SAP SuccessFactors Succession & Development.

SAP Data Encryption supports enterprise infrastructure and HCM ecosystem applications, including payroll, single sign-on, and OpenText solution extensions from SAP. The solution also supports Web services application programming interfaces (APIs) for integration with third-party and on-premise applications.

Boost security with advanced data protection

Preserve critical functionality for protected data

Integrate with other business software



Support data privacy across your entire HCM ecosystem with SAP Data Encryption.



Simplify data privacy compliance and auditing

SAP Data Encryption reduces the cost of data privacy compliance while simultaneously protecting enterprises and safeguarding data assets. By encrypting PII data, the solution separates employees from their HR data. For example, compensation data may be unencrypted, but the solution encrypts the fields that tie an individual to data. This data separation allows companies to significantly reduce the scope of data that needs to be audited, saving both time and money.

Unencrypted personal data is stored within the company firewall. Because employees of cloud

providers cannot decrypt and view PII data, you may not need to include cloud providers in your personal data audit scope.

Better protection and increased transparency of your ability to meet even the most stringent data privacy and residency regulations help you minimize both the cost of compliance and your audit footprint. You can assure employees that their personal data is stored in a secure, unidentifiable way – helping build trust in an interconnected digital world where data breaches are far too common.

Simplify data privacy compliance and auditing



Maximize your investment in HCM solutions while protecting employee data. SAP Data Encryption can show you how.



Summary

The SAP® Data Encryption solution by CipherCloud helps companies in regulated industries extend advanced data protection to their SAP SuccessFactors® solutions. Use it to protect employee data with powerful encryption features while preserving the ability to access critical solution functionality. The solution helps customers meet today's most stringent industry security standards.

Objectives

- Protect sensitive employee data from unauthorized access
- Comply with strict data privacy and regulatory requirements
- Avoid business disruption
- Enable advanced data protection in your solution environment

Solution

- In-line gateway protection to encrypt sensitive employee data and protect it from unauthorized access
- Support for compliance with strict data privacy and regulatory requirements
- Preserved functionality of SAP SuccessFactors solutions for human capital management (HCM)
- Integration of advanced data protection within your HCM solution environment

Benefits

- Enhanced protection of employee personal information
- Prevention of unauthorized access to sensitive data
- Increased value from SAP SuccessFactors solutions for HCM
- More effective compliance with data privacy and residency mandates

Learn more

[Find out](#) how SAP Data Encryption can help you protect employee data and meet regulatory mandates.



Studio SAP | 53219enUS (17/11)

© 2017 SAP SE or an SAP affiliate company. All rights reserved.

No part of this publication may be reproduced or transmitted in any form or for any purpose without the express permission of SAP SE or an SAP affiliate company.

The information contained herein may be changed without prior notice. Some software products marketed by SAP SE and its distributors contain proprietary software components of other software vendors. National product specifications may vary.

These materials are provided by SAP SE or an SAP affiliate company for informational purposes only, without representation or warranty of any kind, and SAP or its affiliated companies shall not be liable for errors or omissions with respect to the materials. The only warranties for SAP or SAP affiliate company products and services are those that are set forth in the express warranty statements accompanying such products and services, if any. Nothing herein should be construed as constituting an additional warranty.

In particular, SAP SE or its affiliated companies have no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation, and SAP SE's or its affiliated companies' strategy and possible future developments, products, and/or platform directions, and functionality are all subject to change and may be changed by SAP SE or its affiliated companies at any time for any reason without notice. The information in this document is not a commitment, promise, or legal obligation to deliver any material, code, or functionality. All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, and they should not be relied upon in making purchasing decisions.

SAP and other SAP products and services mentioned herein as well as their respective logos are trademarks or registered trademarks of SAP SE (or an SAP affiliate company) in Germany and other countries. All other product and service names mentioned are the trademarks of their respective companies.

See <http://www.sap.com/corporate-en/legal/copyright/index.epx> for additional trademark information and notices.