# Table of Contents

4  SAP Supports Global and Local Regulations

5  SAP Enables Physical Security

6  SAP Maintains Network Security

7  SAP Supports Application Security

8  SAP Enables Data Segregation, Limited Data Access, and Encryption

9  SAP Performs Routine Security Audits

10 SAP Demonstrates Corporate Commitment to Security

11 Choosing the Right SaaS HCM Provider
As a cloud provider, SAP is equipped to secure your data even better than you can – and meet regulatory standards better as well. SAP® SuccessFactors® solutions enable best practices for data privacy and cloud security to help you protect your human capital management (HCM) investment. In its November 2016 paper Cloud Security and Data Privacy − Best Practices in HCM Software, global IT analyst firm Neuralytix identifies these best practices, which we discuss in further detail below.

**BEST PRACTICES RECAP**
While some customers may instinctively believe that it is safer to store data on-site, this has not always proven to be the case – as seen in high-profile hacks in the banking and retail industries. To ensure data privacy and cloud security, it’s essential that companies apply best practices when choosing and deploying software solutions.

When choosing a cloud solution for your human capital management (HCM) software, Neuralytix suggests a number of best practices considerations regarding cloud security. The IT analyst firm recommends that cloud software vendors:

- Support global and local regulations
- Enable physical security, including strong perimeter firewalls and defenses
- Maintain network security, including segregated networks
- Support application security
- Enable database security, including limited data access and encryption
- Perform routine security audits
- Demonstrate corporate commitment to security

The following sections provide detail on how SAP and SAP SuccessFactors solutions adhere to these best practices.
SAP Supports Global and Local Regulations

Keeping up with ever-changing regulations is a continuous effort. Each region has a variety of laws and regulations – and the trend for more regulation is only increasing. In the past 4 years alone, we here at SAP have seen an increase of 22% in the number of labor laws and changes issued in the 81 countries that SAP actively tracks. With more than 84,000 employees in over 130 countries, SAP is uniquely qualified to stay on top of these changes.

We are committed to minimizing the burden for our customers of staying legally compliant in all parts of the world. With our significant worldwide presence of over 45 years and support for nearly all countries worldwide, we created two specialized globalization services teams. Our teams work together to secure and enhance the globalization and localization of SAP solutions across our solution portfolio.

GLOBALIZATION SERVICES PRODUCT MANAGEMENT TEAM
Consisting of more than 200 people located in-country – with deep local roots, native language capabilities, and an expert understanding of local regulations and markets – our local product managers analyze local legal requirements and prioritize developments through an established structured process. In many countries, the local product managers collaborate with legislative bodies to guide, test, and implement legal changes, often using established HCM community user groups to assist in the testing process.

GLOBALIZATION SERVICES PRODUCT DEVELOPMENT TEAM
Working with our product management team, more than 300 product developers review, evaluate, prioritize, develop, and implement statutory and legal changes into SAP SuccessFactors HCM Suite solutions.
SAP Enables Physical Security

All SAP data centers comply with telecommunications infrastructure standards, achieving ANSI/TIA-942* Tier III+ and Tier IV ratings, and are certified according to the International Organization for Standardization (ISO) 27001 standard. The data centers provide continuous monitoring. They are equipped with multiple, redundant UPS-protected power circuits with generator backup; smoke detection units; fire suppression systems; 24x7 year-round on-site security personnel; and intrusion-detection alarm systems.

Illegal entry is blocked with the help of biometric readers, bulletproof walls, and concrete pillars. Data center access is restricted to authorized SAP personnel only; extensive background checks are required. Access is logged, monitored, and requires multifactor authentication – including photo IDs, key cards, personal ID numbers (PIN), and biometric authentication – and other measures to prevent equipment and data center facilities from being compromised.

Two specialized globalization services teams work together to secure and enhance the globalization and localization of SAP solutions across our solution portfolio.
SAP Maintains Network Security

SAP uses a multitier network architecture and limits end-user traffic to the front tier, or “demilitarized zone” (DMZ), of Web servers. A firewall-controlled, segregated virtual local area network (VLAN) isolates each tier of the network system from the other tiers, and each tier is set up on its own hardware stack. All requests are validated individually before independent requests to the next tier are generated. Incoming user requests pass through the firewall down to the load balancers, and load balancers distribute the traffic to the appropriate Web server for processing. The Web server then makes independent requests to the application tier, and the application tier makes independent requests to the database tier.

At each level, the incoming request is validated against business and security rules to protect against malicious access. Requests that fail validation are terminated. Traffic within each tier is restricted. Only required ports are enabled on servers and permitted between VLANs. The firewall separating the application and database tiers uses a default policy that drops all traffic unless specifically required. Unique to SAP, our patented technology deployed between the application and database firewall prevents Structured Query Language (SQL)—injection attacks and cross-site scripting attacks.

Security is reinforced with connections to multiple tier 1 Internet service providers (ISPs) for highly available network access. All network equipment is redundant, providing automatic failover between devices. Web, application, and database tiers are configured as secure segments and are tuned for maximum performance.

Local product managers analyze local legal requirements and prioritize developments through a structured process and collaborate with legislative bodies to guide, test, and implement legal changes.
SAP Supports Application Security

SAP SuccessFactors solutions employ extensive security measures to protect against the loss, misuse, and unauthorized alteration of data. Our solutions help you achieve the following:

- **Protect applications from insider threats**, with tight encryption through a 256-bit Secure Sockets Layer (SSL) connection. Using open standards (HTML and JavaScript) helps ensure that applications do not require any changes or special permissions on a user’s desktop.

- **Avoid risky plug-ins and downloads** that can cause viruses or other threats by using browser-based administrative functions, such as password resets.

- **Guard against “phishing” and “pharming”** by using e-mail encryption and regular virus scans, as well as plain-text e-mails, to eliminate the possibility of a hidden link that can gather information from users.

- **Protect against improper logins** by requiring user logins each time the application is opened, by using one-way Secure Hash Algorithm 1 (SHA-1) hash encrypted passwords, and by using automatic logouts after 30 minutes and account locks after multiple failed logins.

- **Provide best practice security at all levels** – function, transaction, field, and data – by using role-based permissions.

- **Enforce segregation of duties** by ensuring that no individual can breach security through dual privileges. No person can hold a role that exercises audit, control, or review authority over another concurrently held role.

SAP SuccessFactors solutions employ extensive security measures to protect against the loss, misuse, and unauthorized alteration of data.
SAP Enables Data Segregation, Limited Data Access, and Encryption

SAP SuccessFactors solutions support a multitenant model that allows for true segmentation of customer data at the database level. Many software as a service (SaaS) vendors employ multitenant systems that use a single database to store data from several customers, separating each data set logically using a primary key such as a company identifier. Unfortunately, this method comingles customers’ data.

SAP uses a different approach with SAP SuccessFactors solutions that separates customer data at the database tier. With SAP SuccessFactors solutions, customer data is segmented logically at the database level, complete with its own database schema. SAP SuccessFactors solutions also provide a distinct application instance per customer, offering better security through enforced memory segregation.

SAP controls all access to information-processing facilities and business processes according to business and security requirements. In all cases, the concept of “least privilege” determines computer access. Users are limited to the minimum set of privileges needed to perform the required function. We classify all information, regardless of medium or form, to reflect its level of confidentiality or importance to SAP and our customers. We classify all customer data as confidential.

SAP SuccessFactors solutions contain advanced security mechanisms, which secure data while at rest, in transit, and in use, and secure access to the data. SAP data centers and SAP SuccessFactors solutions adhere to the following standards:
- ISO 27001
- British Standard 10012
- Statement on Standards for Attestation Engagements (SSAE) 16 and International Standard on Assurance Engagements (ISAE) 3402
- Service Organization Controls (SOC) accounting standard SOC 2
- U.S. government Federal Information Security Management Act (FISMA) standards

SAP SuccessFactors solutions encrypt data in a way that doesn’t affect applications. The solutions decrypt the data on the fly when applications access the data, but they keep the data encrypted for other types of access. The solutions use a minimum of Advanced Encryption Standard (AES) 256–bit encryption to secure data at the block level of the storage systems for SAP SuccessFactors solutions. Key managers for SAP SuccessFactors solutions have passed the Federal Information Processing Standard (FIPS) 140-2 level 3 certification testing.

SAP data centers run full and incremental data backups weekly and full archive log backups daily. SAP maintains three copies of customer data, for unmatched redundancy: original, primary backup, and replicated or clone copy. Backed-up data is encrypted at the AES 256–bit level, for data at rest and data in motion. This data is available for rapid reimplementation and system restores if the original data becomes corrupt.
**SAP Performs Routine Security Audits**

Penetration testing protects system security against exploits and vulnerabilities. SAP performs daily application vulnerability testing and brings in independent third-party professional specialists for quarterly penetration testing. SAP also conducts regularly scheduled infrastructure scans and allows customers to optionally conduct their own penetration testing.

SAP performs regular database audits to maintain records that demonstrate proof of origin; all alterations, additions, and deletions; the date and time stamp of a data change; and approvals where appropriate. To maintain an audit log’s viability, the log is unalterable, encrypted, and kept on a network segment to which system engineers do not have access.

Unlike most SaaS vendors, who perform annual audits, SAP completes the SSAE 16 and SOC 2 compliance audit report every 6 months. Customers can request copies of these audit reports from their account executives.
SAP Demonstrates Corporate Commitment to Security

We have been delivering SaaS solutions for over 15 years. We take a global and comprehensive approach to security. SAP has received 11 security patents to date – and we continue to innovate in this area. SAP has an established data protection and privacy team that consists of attorneys, auditors, privacy, and technical experts. The team’s core responsibilities include the shaping of SAP’s data protection policies and standards, providing advice, recommending key compliance measures, monitoring compliance, conducting audits, training staff, and incident response.

To provide truly global services, our data protection and privacy team maintains a worldwide network of data protection and privacy coordinators, one in each line of business and/or legal entity. Our coordinators provide input from other jurisdictions and they help the data protection and privacy team to implement data protection and privacy requirements across SAP. Thus, they help maintain the data protection compliance of SAP products and services.

In addition, every year, SAP invests more than €500,000 to audit the SAP Cloud portfolio. This expenditure is necessary to meet the legally mandated audit-assistance obligation for cloud providers.

Every year, SAP invests more than €500,000 to audit the SAP Cloud portfolio.
Choosing the Right SaaS HCM Provider

In addition to the best practices and checklist items discussed above, customers should ensure their SaaS-based HCM provider has experience in providing secure IT environments, understands the challenges of your industry, and operates in the same countries and regions you do. The right combination of deployment models and best practices can help IT meet your data privacy and security challenges.

With SAP SuccessFactors solutions, SAP is uniquely qualified as a SaaS-based provider of HCM software. In addition to the broad expertise described previously, we also draw on more than 15 years of experience delivering SaaS solutions, and we’ve served more than 6,200 customers of all sizes in more than 60 industries and 177 countries.

LEARN MORE
For more information on SAP SuccessFactors solutions, visit www.successfactors.com. To take a comprehensive tour of a data center, visit www.sapdatacenter.com.