

No. 16

SAP HCM

HR and Payroll Security

Protecting employee and payroll data in SAP HCM for SAP S/4HANA and SAP SuccessFactors, explained for beginners

oJAYo.com

oJAYo

FREE SAMPLE · ojayo.com

SECTRAININGNOW SERIES · NO. 16

HR and Payroll Security

Protecting employee and payroll data in SAP HCM for SAP S/4HANA and SAP SuccessFactors, explained for beginners

oJAYo
Published by oJAYo.com

FREE SAMPLE · ojayo.com

HR and Payroll Security
Protecting employee and payroll data in SAP HCM for SAP S/4HANA and SAP SuccessFactors, explained for beginners

First edition, 2026. Copyright © 2026 oJAYo. Published by oJAYo.com. All rights reserved. No part of this book may be reproduced or shared without written permission, except for brief quotations in reviews.

This book is an independent publication. SAP, SAP S/4HANA, SAP Fiori, SAP Gateway, SAP BTP, SAP Build Work Zone and other SAP products mentioned are trademarks or registered trademarks of SAP SE in Germany and other countries. All other product names are trademarks of their respective owners. oJAYo.com is not affiliated with, sponsored by or endorsed by SAP SE or any other vendor named in this book.

The information in this book is provided for education. Product features change between releases; always confirm details in the official documentation for your release before changing a production system. Screens marked “Illustration” are simplified drawings, not captures of real SAP software. Company and person names in examples are fictional.

[ISBN: add if registered]

FREE SAMPLE · ojayo.com

CONTENTS

How to use this book 1

PART I · FOUNDATIONS

1 Why HR and payroll data needs special care 5

2 The SAP HR landscape today 9

3 How HR authorization checks work 13

PART II · BUILDING HR ACCESS

4 General authorizations: P_ORGIN and friends 20

5 Payroll authorizations 26

6 Structural authorizations 30

7 Employee and manager self-service 35

PART III · PROTECT AND MONITOR

8 Critical access and bypasses 40

9 Privacy, logging and data protection 45

10 Segregation of duties in HR and payroll 49

11 SAP SuccessFactors and Employee Central Payroll 53

PART IV · OPERATE

12 Troubleshooting HR access 59

13 Reviews and checklists 62

14 Worked cases 66

Glossary 70

Further reading 72

FREE SAMPLE · ojayo.com

BEFORE YOU BEGIN

How to use this book

What this book covers, who it is for, and how to use it.

Salaries, bank accounts, home addresses, health-related absences, performance ratings, national ID numbers: HR and payroll systems hold the most personal data a company has. A single over-generous role can let someone read the pay of the whole company or change their own bank details before payday.

This book explains **how SAP protects HR and payroll data**, and how you can set up, review and troubleshoot that protection, written for beginners.

Which SAP products this book covers

SAP's HR landscape is changing. The book focuses on what is current:

- **SAP HCM for SAP S/4HANA** (often shortened to **H4S4**), the on-premise HR and payroll solution that runs on SAP S/4HANA, including SAP S/4HANA Cloud Private Edition. It was shipped with the SAP S/4HANA 2022 release, and partners report SAP's maintenance commitment to the end of 2040.
- **SAP SuccessFactors Employee Central** and **SAP SuccessFactors Employee Central Payroll**, SAP's cloud HR suite.

Two older setups are still in use and are treated as **legacy** here:

- **SAP ERP HCM on SAP ECC 6.0**: widely published dates give mainstream maintenance until the end of 2027, with optional extended maintenance to the end of 2030.
- **The HCM compatibility pack inside SAP S/4HANA**: its usage rights ended at the end of 2025, and customers were expected to move to H4S4 or to the

FREE SAMPLE · ojayo.com

cloud.

The good news for security teams: the **HR authorization concept** (P_ORGIN, P_PERNR, structural authorizations and the rest) works the same way in SAP HCM for SAP S/4HANA as it did in SAP ERP HCM. What you learn here applies to both, while SuccessFactors uses a different model, covered in Chapter 11.

> **WATCH OUT**
> Maintenance and licensing dates come from SAP announcements and can change. Always check SAP's current information for your own contract before planning.

Who this book is for

- **SAP security analysts** who are asked to build or fix HR roles for the first time.
- **HR and payroll IT teams** who own HR systems.
- **Auditors and data protection officers** reviewing who can see personal data.
- **HR managers** who approve access to their teams' data.

How the book is organized

- **Part I — Foundations** (Chapters 1–3): why HR data needs special protection, the HR landscape, and how HR authorization checks differ from other SAP checks.
- **Part II — Building HR access** (Chapters 4–7): general authorizations, payroll authorizations, structural authorizations, and self-service.
- **Part III — Protect and monitor** (Chapters 8–11): critical access and bypasses, data privacy and logging, segregation of duties, and SAP SuccessFactors.
- **Part IV — Operate** (Chapters 12–14): troubleshooting, reviews and checklists, and worked cases.

FREE SAMPLE · ojayo.com

Conventions

TIP

Practical advice you can apply straight away.

IN SAP

Product-specific details, such as transactions, tables and authorization objects.

WATCH OUT

Common mistakes and risks.

KEY IDEA

The one thing to remember from a section.

A note on screens and examples

The screens in this book are **simplified illustrations**, drawn to explain ideas. They are not copies of SAP screens. All names, personnel numbers, organizational units and values are invented. HR data is personal data: when you practise, use a test system with fictitious or anonymised employees, never real records.

FREE SAMPLE · ojayo.com

PART I

Foundations

HR security is not just ordinary SAP security with different object names. These chapters explain what is at stake, which SAP HR options exist today, and how HR authorization checks are built.

FREE SAMPLE · ojayo.com

CHAPTER 1

Why HR and payroll data needs special care

Most SAP data belongs to the company. HR data belongs, in a very real sense, to the people it describes. That changes how it must be protected.

What an HR system knows

A typical SAP HR system stores, for every employee:

- **identity data** — name, date of birth, national ID or tax numbers, nationality;
- **contact data** — home address, private phone, emergency contacts;
- **employment data** — position, organizational unit, manager, contract type, working time;
- **pay data** — basic pay, bonuses, deductions, garnishments, payroll results for many years;
- **bank data** — accounts used for salary payments;
- **time and absence data** — including absence types that may reveal health or family situations;
- **performance and talent data** — ratings, objectives, succession plans.

Many of these items are **special categories** or highly sensitive data under privacy laws such as the EU General Data Protection Regulation (GDPR). Even where a law does not label them, employees reasonably expect them to stay private.

FREE SAMPLE · ojayo.com

What can go wrong

HR security incidents are often not dramatic hacks. They are everyday access that is simply too wide:

- an HR clerk in one country can see the salaries of executives worldwide;
- a payroll administrator can change their own bank details or basic pay;
- a manager can see the data of a whole division, not only their team;
- a support consultant downloads a table with all employees' bank accounts "for analysis";
- a test system refreshed from production contains real salaries, and dozens of developers can read them;
- a fraudulent "ghost employee" is hired and paid by one person who controls both steps.

KEY IDEA

In HR, **read access is a risk on its own**. In many SAP areas, the main concern is who can change data. In HR, who can **see** data is just as important.

Who needs what

Different people need very different slices of HR data:

Person	Needs	Should not have
Employee	Own address, bank details, pay statements	Colleagues' data
Manager	Team's basic data, absences, some talent data	Salaries outside the team, unrelated divisions
HR administrator	Master data for assigned employees	Executive pay, own record changes
Payroll administrator	Pay infotypes and payroll runs for assigned payroll areas	Hiring, bank data changes plus payment release
HR IT / security	Configuration, roles	Day-to-day access to salaries

FREE SAMPLE · ojayo.com

Translating this table into SAP roles is the work of the rest of this book.

Why standard SAP roles are not enough

General SAP authorization objects decide whether a user may start a transaction or post in a company code. For HR, that is far too coarse. SAP therefore built an **HR-specific authorization concept** that can decide:

- **which infotypes** (data groups such as address, basic pay or bank details) a user may access;
- **for which employees**, based on their organizational assignment or position in the org structure;
- **at which level**: read, write, or only search;
- **for which time period**.

Chapter 3 introduces this concept.

Legal and audit expectations

Regulators, works councils and auditors commonly expect:

- **need-to-know access** to personal data, documented and approved;
- **segregation of duties** in payroll, especially between master data and payment;
- **logging** of access to the most sensitive data;
- **deletion or blocking** of personal data after retention periods;
- **protection of non-production systems**, which must not become an uncontrolled copy of production.

The exact requirements depend on your countries and industry. Involve your data protection officer and, where applicable, employee representatives when you design HR access.

Summary

- HR systems hold the most sensitive personal data in the company.

FREE SAMPLE · ojayo.com

- Read access is a risk on its own.
- SAP has an HR-specific authorization concept for infotypes, employees, levels and time.
- Legal and audit expectations cover need-to-know access, SoD, logging, deletion and test systems.

FREE SAMPLE · ojayo.com

The oJAYo library

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

SAP SECURITY · 67 BOOKS

SAP Role Design Handbook
Access Control Field Guide
Signavio Process Governance
ABAC in Practice
Auditing SAP Systems
Securing SAP BTP
Securing SAP Fiori
SAP User Training Playbook
SAP Basis Essentials
SAP HANA Security
SAP Authorization Troubleshooting
HR and Payroll Security (you are reading this)
Finance and Procurement Authorizations
BW and BusinessObjects Security
SAP Network and Web Security
SAP Security Interview Guide
SAP Cloud ALM Security
SAP Data Services Security
SAP Architecture Explained
SAP SD Security
SAP CRM Security
SAP SRM Security
SAP Ariba Security
SailPoint for SAP
SAP PP Security
SAP QM Security
PI/PO and Integration Suite Security
SAPUI5 Security
Testing in SAP Cloud ALM with Jira
SAP SLT Security
SAP PS Security
SAP Plant Maintenance Security
SAP EWM Security
SAP Digital Manufacturing Security
SAP SuccessFactors Security
Security in SAP Activate
SAP Concur Security
SAP Fieldglass Security
SAP Analytics Cloud Security
SAP Datasphere and Business Data Cloud Security
SAP Build and Work Zone Security
Joule and SAP Business AI Security
SAP MDG Security
SAP TM Security
SAP IBP Security
SAP GTS Security
SAP Sales, Service and Commerce Cloud Security
SAP S/4HANA Cloud Public Edition Security
SAP Business One and ByDesign Security
SAP Identity Management Migration
SAP Security Patching
Threat Detection and SIEM for SAP
Data Privacy (GDPR) for SAP
RISE with SAP Security
Ransomware and Incident Response for SAP
Compliance Mapping for SAP
Third-Party and Support Access for SAP
SAP Process Control and Risk Management
SAP Cloud Identity Access Governance
SAP Cloud Identity Services
SAP System Hardening
SAP Certificates and Encryption
SAP Penetration Testing
SAP Security Roadmap
Secure Development on SAP BTP
SAP Data Custodian and Data Sovereignty
Threat Intelligence for SAP

CYBERSECURITY · 64 BOOKS

Zero Trust Networks
Productivity at Work
ABAP Custom Code Security
S/4HANA Conversion Role Redesign
Getting Started with Canva AI
Getting Started with Character.AI
Getting Started with DeepL
Getting Started with Perplexity
Prompt Engineering
Cybersecurity Basics
Python for Beginners
JavaScript for Beginners
DevOps and Platform Engineering
AI-Powered Cyber Attacks
Securing AI Agents and Shadow AI
Ransomware
Phishing and Social Engineering
Deepfakes and Identity Fraud
Post-Quantum Cryptography
Software Supply Chain Security and DevSecOps
OT and Industrial Security
Sovereign Cloud and Data Sovereignty
Geopolitical Cyber Risk
Cloud Security and Identity Protection
Identity and Access Management Basics
Privileged Access Management
Passwordless and Passkeys
Identity Threat Detection and Response
SSO and Federation
AWS Security Fundamentals
Microsoft Azure and Entra ID Security
Google Cloud Security
Kubernetes and Container Security

FREE SAMPLE · ojayo.com

The oJAYo library (continued)

170 plain-language PDF books · $49 each · free sample of every book at ojayo.com

Cloud Security Posture Management
Serverless Security
OWASP Top 10 for Web Applications
API Security
Secure Coding Practices
Threat Modeling
Mobile App Security
SOC Fundamentals
Incident Response Planning
Digital Forensics
Threat Hunting
EDR and XDR
Malware Analysis Basics
Ethical Hacking for Beginners
Red Teaming and Purple Teaming
Bug Bounty Hunting
CTF for Beginners
Data Loss Prevention
Encryption Basics
Privacy Engineering and Privacy by Design
Data Classification and Governance
NIST CSF 2.0
ISO 27001
SOC 2 for Startups
PCI DSS 4.0
HIPAA Security for Healthcare
Third-Party and Vendor Risk Management
Email Security: DMARC, SPF and DKIM
IoT and Smart Device Security
Cyber Insurance
Security Awareness Training Programs

AI · 11 BOOKS

Working with Claude
Working with ChatGPT
Getting Started with Google Gemini
Getting Started with DeepSeek
Getting Started with Grok
Getting Started with Microsoft Copilot
Agentic AI Explained
MCP: The Model Context Protocol
Vibe Coding
AI Coding Tools
AI Detection

CERTIFICATION GUIDES · 28 BOOKS

CompTIA Security+ Study Guide
ISC2 CC Study Guide
ISC2 CISSP Study Guide
ISACA CISM Study Guide
ISACA CISA Study Guide
ISACA CRISC Study Guide
ISC2 CCSP Study Guide
CompTIA CySA+ Study Guide
CompTIA PenTest+ Study Guide
EC-Council CEH Study Guide
OffSec OSCP+ Study Guide
CompTIA SecurityX Study Guide
GIAC GSEC Study Guide
AWS Certified Security - Specialty Study Guide
Microsoft Security Certifications Study Guide
CompTIA SecAI+ Study Guide
ISACA AAISM Study Guide
ISACA AAIA Study Guide
ISACA AAIR Study Guide
IAPP AIGP Study Guide
ISO/IEC 42001 Lead Implementer and Lead Auditor…
AWS Certified AI Practitioner Study Guide
AWS Certified Machine Learning Engineer - Associ…
AWS Certified Generative AI Developer - Profession…
Microsoft AI-901 Study Guide
Microsoft AI-103 Study Guide
Google Cloud Generative AI Leader Study Guide
Google Cloud Professional Machine Learning Engin…

BUNDLES · 18 PACKS, SAVE UP TO $145

SAP Security Starter Pack (5 books, $149)
SAP GRC and Audit Pack (5 books, $129)
S/4HANA Migration Security Pack (4 books, $109)
SAP Cloud Security Pack (5 books, $129)
SAP Threat Defense Pack (5 books, $129)
Cybersecurity Starter Pack (5 books, $129)
Identity and Access Pack (5 books, $129)
Cloud Security Pack (6 books, $149)
SOC and Incident Response Pack (5 books, $129)
Application Security Pack (5 books, $129)
Security Compliance Pack (5 books, $129)
Ethical Hacking Pack (5 books, $129)
AI at Work Pack (5 books, $129)
AI Developer Pack (5 books, $129)
AI Security and Governance Pack (5 books, $129)
CISSP + Security+ Exam Pack (2 books, $79)
ISACA Exam Pack (3 books, $99)
AI Certification Pack (4 books, $109)

END OF FREE SAMPLE

HR and Payroll Security

Enjoyed it? The full book has 77 pages and 14 chapters.
Instant PDF download, $49.

Get the full book

ojayo.com · Created by the oJAYo expert team

This sample may be shared freely. The full book is licensed to one reader.