



Navigating Payroll Compliance in a Changing Data Privacy Landscape

Brett Corbett, HCM Solutions Lead, EPI-USE Labs

Introduction



Brett Corbett

HCM Solutions Lead, EPI-USE Labs

Brett.Corbett@labs.epiuse.com

- **17+ years** in SAP HR/Payroll, specialising in global rollouts and large-scale implementations.
- Expertise in **SAP/SuccessFactors HCM, data management, and payroll reporting solutions.**
- Solution lead for **EPI-USE Labs' Data Sync Manager, Query Manager, and Variance Monitor** implementations.



Agenda

- The importance of payroll data protection
- Navigating key data protection laws
- What happens when compliance fails?
- The true cost of a data breach
- Essential practices for protecting your payroll data



Data protection in payroll

Why it should be a top priority for New Zealand organisations

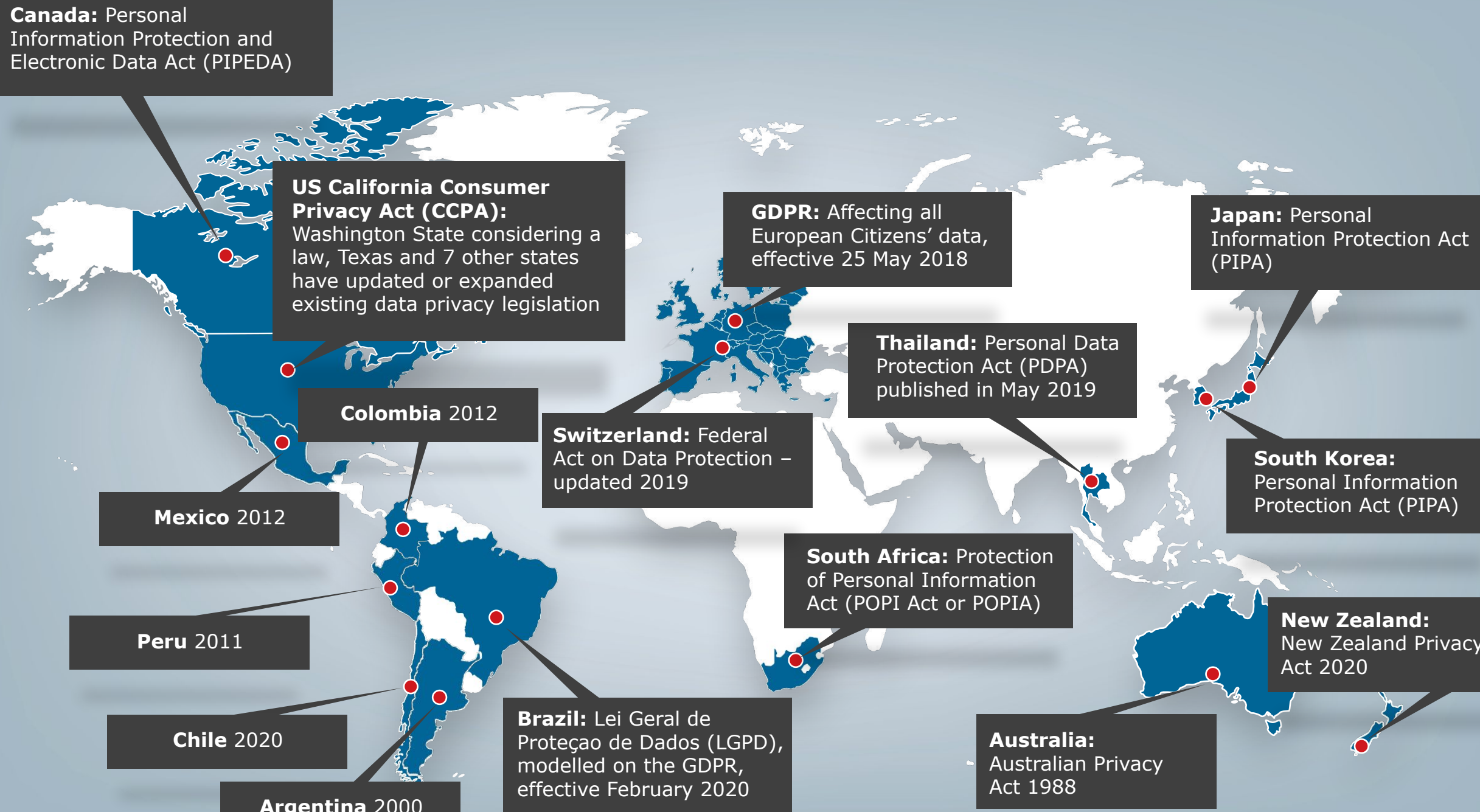
- Payroll data is personal data
- Protecting employee trust is critical
- Risks of breach extend beyond fines

The real cost of a data breach

- **Reputation:** A breach can cause lasting PR damage
- **Employee trust:** Loss of talent & morale
- **Financial impact:** legal costs, fines and more





A world map with a light blue background. Countries are outlined in white. A set of countries, including Canada, the United States, Mexico, Colombia, Peru, Chile, Argentina, Brazil, Switzerland, Germany, France, the United Kingdom, Thailand, South Africa, Australia, New Zealand, Japan, and South Korea, are highlighted in a darker blue. Red circular markers are placed on each of these highlighted countries. Black lines (callouts) connect each red marker to a black rectangular text box containing information about data privacy legislation in that country. The text boxes are arranged around the map, generally following the geographical distribution of the highlighted countries.

Canada: Personal Information Protection and Electronic Data Act (PIPEDA)

US California Consumer Privacy Act (CCPA):
Washington State considering a law, Texas and 7 other states have updated or expanded existing data privacy legislation

GDPR: Affecting all European Citizens' data, effective 25 May 2018

Japan: Personal Information Protection Act (PIPA)

Thailand: Personal Data Protection Act (PDPA) published in May 2019

Colombia 2012

Switzerland: Federal Act on Data Protection – updated 2019

South Korea: Personal Information Protection Act (PIPA)

Mexico 2012

South Africa: Protection of Personal Information Act (POPI Act or POPIA)

Peru 2011

New Zealand: New Zealand Privacy Act 2020

Chile 2020

Australia: Australian Privacy Act 1988

Argentina 2000

Brazil: Lei Geral de Proteção de Dados (LGPD), modelled on the GDPR, effective February 2020



Key data protection laws you need to know

Navigating data protection laws in New Zealand

- Privacy Act 2020: Your responsibility to protect data
- GDPR (General Data Protection Regulation)





Privacy Act 2020

What you need to know

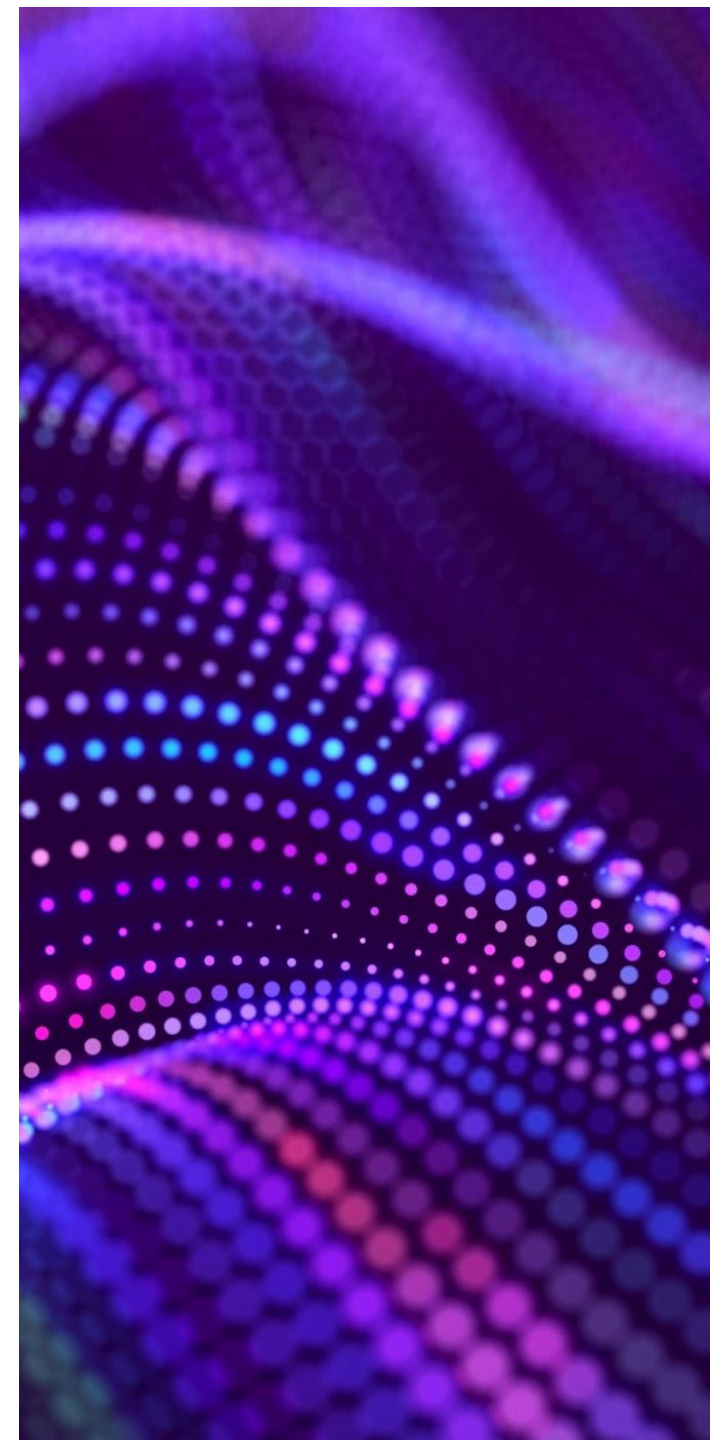
- **Payroll implications:** Protects personal data, including payroll information, for individuals in New Zealand
- **Key requirements:**
 - **Transparency & Consent:** Employees must know what payroll data is collected and why
 - Data security: Payroll records must be securely stored and protected from unauthorised access
 - **Right to access & correction:** Employees can request access to their payroll data and have errors corrected
 - Breach notification: **Serious data breaches must be reported to the Privacy commissioner**
 - Personal data stored offshore must be protected to NZ standards
- **Penalties:**
 - Fines of \$10,000 (individuals) and \$50,000 (organisations) for serious breaches
 - Highest so far - \$168,000



GDPR

The global push for stronger data protection

- **About the GDPR**
 - Introduced in 2018, setting the global benchmark for data privacy laws
 - Applies to any business handling EU citizen's personal data, even outside the EU
 - Many countries are adopting similar principles, so it's only a matter of time before the same rules apply to New Zealand citizens.
- **GDPR follows similar principles to the NZ privacy act 2020, but with extra conditions:**
 - **Right to be forgotten:** Employees can request payroll data deletion unless legally required to retain it
 - **Explicit consent for processing:** Payroll teams must document why they collect and process data
 - **Data portability:** Employees can request payroll data in a structured format to transfer to another employer
 - **Stricter breach reporting:** Must notify authorities within 72 hours of a payroll data breach
 - **Higher penalties:** Fines up to \$20M pounds or 45% of annual revenue for non-compliance





GDPR

The global push for stronger data protection

- **Why this matters**
 - If processing payroll for EU-based employees, your company must comply with GDPR
 - NZ privacy laws are evolving toward stronger protections – this could be a future requirement
 - International payroll providers may already align with GDPR to meet compliance across markets

SAP Security road to compliance

Impact and risk assessment
– Identify your risks

SE16 TABLE EXPORTS SITTING IN C:\TEMP



Find and map your PII



Review access and controls risk



Clean up the backlog in production

Manage sensitive data in Production copies

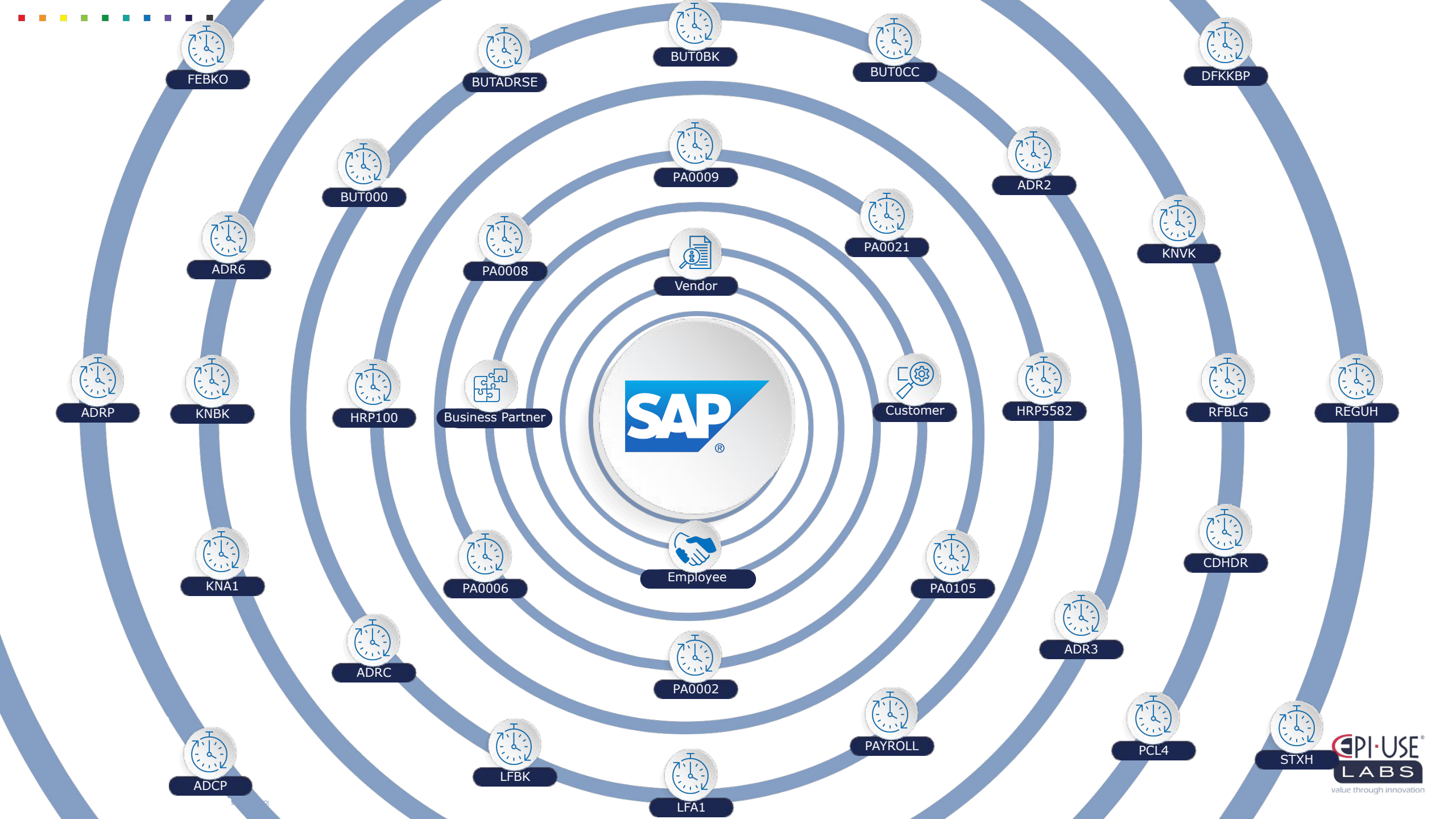
SE16 TABLE EXPORTS SITTING IN C:\TEMP



imgflip.com

The background is a solid blue color with a subtle pattern of white geometric shapes, including squares, circles, and lines, scattered across the surface. The text is centered in the upper half of the image.

I've been running SAP for 15 years now; how much
Personally Identifiable Information (PII) do I have?





Details of Sync: ██████████-0000018

Menu ▾ ▾ ◀ Back CLOSE Cancel System ▾ Refresh Documentation

Overview Object tree Statistics Default level audit Calculation audit (key level) Update audit (field level) Messages

       Display 200 records ▾ 

System	Old Value	New Value	Integrity Map (ID)	Table Name	Field Name	Table Key	Deleted
100	833-20	833-20	PA0009_BANKL	PC209	BANKL	833-20	<input type="checkbox"/>
100	833-20	833-20		PA0009	BANKL	100,10001,0,,99991231,20201031,000	<input type="checkbox"/>
100	833-20	833-20		PA0009	BANKL	100,10001,2,,99991231,20201128,000	<input type="checkbox"/>
100	207830	9999990	PA0009_BANKN	PC209	BANKN	207830	<input type="checkbox"/>
100	207830	9999990		PA0009	BANKN	100,10001,0,,99991231,20201031,000	<input type="checkbox"/>
100	207830	9999990		PA0009	BANKN	100,10001,2,,99991231,20201128,000	<input type="checkbox"/>
100	T	T	PA0009_ZLSCH	PC209	ZLSCH	T	<input type="checkbox"/>
100	T	T		PA0009	ZLSCH	100,10001,0,,99991231,20201031,000	<input type="checkbox"/>
100	T	T		PA0009	ZLSCH	100,10001,2,,99991231,20201128,000	<input type="checkbox"/>
100	207830	9999990	PAYMENTINFORMATION	PaymentInformationDetailV3	ACCOUNTNUMBER	207830	<input type="checkbox"/>



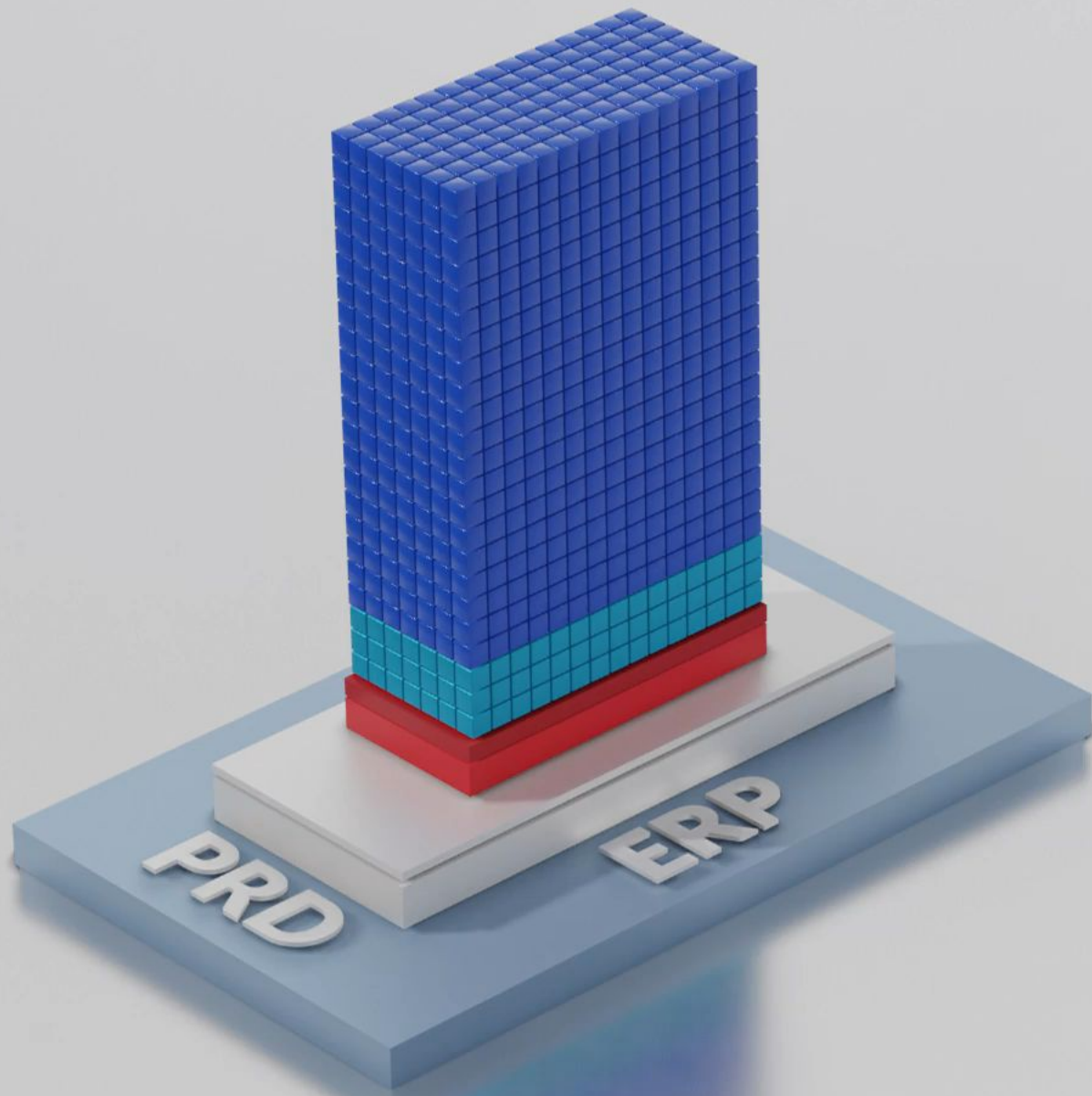
Data Discovery

Technical Discovery and Workshop consulting

At EPI-USE Labs, we leverage our unique, market-leading IP containing defined mapping of data throughout SAP in finding additional related PII in your instance.

Separate to the Data Sync Manager software, Data Discovery is applied to your production environment and executed to check the Dictionary for custom tables with PII, and check the contents of these tables.





Data privacy workshop and system analysis

- A collaborative workshop followed by an in-depth system analysis
- A small professional services engagement requiring around one week of effort:
 - One day of workshops
 - Three days' system analysis
 - A final day preparing the output report
- Providing SAP solution expertise, with a background of implementing privacy projects in multiple industries throughout the globe. We can help mediate functional, compliancy and testing needs with real examples and impacts to lead to a clear requirement moving forward.
- After the analysis, you will be presented with a detailed report which outlines:
 - Production and non-production privacy requirements
 - Retention process flows
 - SAP object definitions and integrations of data
 - Cross system integrations and data alignments
 - Detailed table and field analysis showing the Personally Identifiable information in you SAP environment.





Data Disclose™



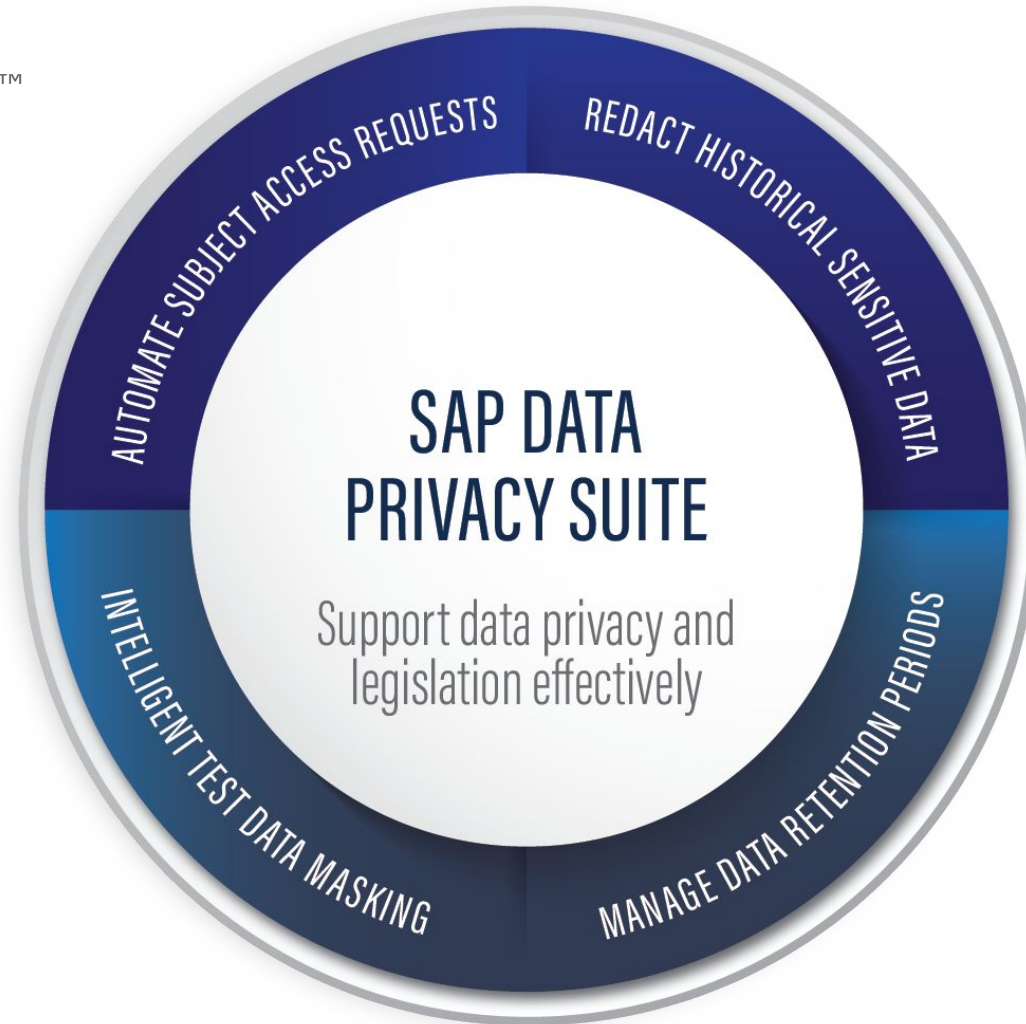
Data Redact™



Data Secure™



Data Retain™





Data Secure

Avoid sensitive data falling into the wrong hands

- Comprehensive data protection solution which masks sensitive data in non-production SAP systems
- Able to consistently scramble data between multiple SAP and non SAP platforms
- Out-of-the box content, mapping the common PII locations within standard SAP in a delivered policy, launched with minimal implementation effort
- Modifiable to include additional custom configuration and system connections to meet your privacy needs
- Mask an entire SAP client for testing or training purposes
- No external connectivity required; data is processed within SAP without additional middleware or transfer of data
- Can be used in place independently, or combined with the DSM data copy facilities to scramble before export from Production
- **Recent addition** – Now with SuccessFactors Employee Central OData API connector option



Data Disclose™

Leveraging trusted technology

Instantly search an SAP landscape to locate, retrieve and present a subject's data footprint with an encrypted PDF download.

Benefits:

Automated, fast search across all ABAP systems (ERP, CRM, HCM, SRM, BW) including non-SAP systems via predefined APIs.

SAP® Certified
Integration with SAP S/4HANA®

SAP® Certified
Integration with SAP S/4HANA® Cloud





Data Redact™

Intelligently alter or clear sensitive or personally identifiable data in SAP systems without removing the complete record, while ensuring referential integrity is not at risk.

Benefits:

Reporting of non-sensitive data is not affected. Comply with legislation requiring the removal of data, without costly archiving or custom deletion solutions.

SAP® Certified
Integration with SAP S/4HANA®

SAP® Certified
Integration with SAP S/4HANA® Cloud





Data Retain™

Proactively find data subjects for redaction based on a set of flexible rules which can be automatically scheduled or run manually, based on your compliance needs.

Benefits:

Keep your systems compliant and get ahead of erasure requests with a standard policy response.

SAP® Certified
Integration with SAP S/4HANA®

SAP® Certified
Integration with SAP S/4HANA® Cloud

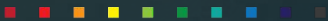




Key areas of action

1. Remove real personal data from test and development systems – both SAP and SuccessFactors
2. Identify and map the PII data in your SAP/SF instance
3. Identify and summarise the PII data held for a Data Subject into a formatted PDF
4. Removal of personal data in production when no longer justified to hold





QUESTIONS

www.epiuselabs.com | sales@labs.epiuse.com | clientcentral.io

LINKEDIN: EPI-USE Labs | TWITTER: @EPIUSELabs | FACEBOOK: EPI-USE Labs



Q&A and next steps

- **Book a free data health assessment today using the QR code.**