

JD Edwards EnterpriseOne and Data Privacy

The Implications of GDPR
& CCPA

Remember to provide your session feedback in the app!

Session ID:

Quest2020-114220

Prepared by:

Colin Dawes
Chief Solution Architect
Syntax

Mike Ward
CEO
Q Software

10th June 2020



Abstract

- The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy for all individuals within the European Union and addresses the export of personal data outside the EU. For global organizations running JD Edwards EnterpriseOne this may have some impact on your topology of instances and environments, application security, requirement for encryption and overall systems management.
- Our focus in this session will be to outline the general implications of the GDPR on your E1 deployment under different scenarios and to provide guidance on the considerations to ensure compliance.
- Using real customer examples and reviewing available tools, we will provide attendees with the overview necessary to begin or further their GDPR implementation.

Objective 1

- Review the GDPR and the impact on EnterpriseOne and suggestions for compliance through topology, instance changes, process changes and security changes.

Objective 2

- Review tools which can aid compliance and monitoring with the GDPR.



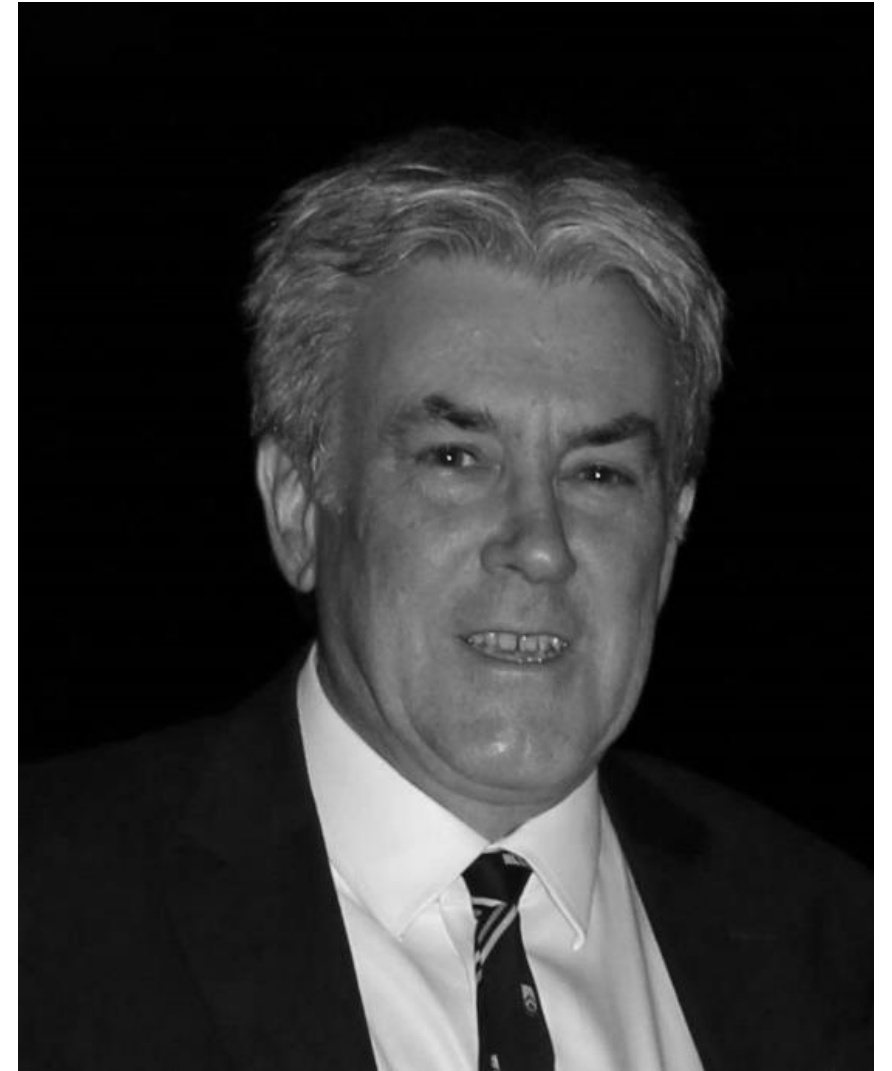
Colin Dawes

- Strategic and innovative technology leader
- 20+ year of IT experience encompassing ERP, Cloud, Mobility, Enterprise Architecture
- Expert on all supported EnterpriseOne databases and platforms
- Performed over 60+ EnterpriseOne installs, upgrades and migrations
- Consulting engagements with over 200 EnterpriseOne customers



Mike Ward

- 45 Years IT Experience
- ERP from the Beginning
- 250 ERP Audits
- A European



Privacy Legislation Overview

JD Edwards EnterpriseOne
and Data Privacy



Privacy Legislation



Acronym	Description	Effective	Applicable To	Applies To
PIPEDA	The Personal Information Protection and Electronic Documents Act	April 13, 2000	All businesses that operate in Canada	All businesses that handle personal information
GDPR	General Data Protection Regulation	May 28, 2018	All individuals within the European Union (EU) and the European Economic Area (EEA)	Anyone who processes the personal data of EU individuals
CCPA	California Consumer Privacy Act of 2018	Jan 1, 2020	California Residents	Anyone who processes the personal data of California residents



The Personal Information Protection and Electronic Documents Act (PIPEDA – Canada)

- All Businesses trading in Canada (since 2000)
- Alberta, BC & Quebec are exempt but have similar Regulations
- Right to Know what Data collected



- Appropriate Security in Place
- Consent to Use PI
- Ombudsman presides over Complaints
- Less Stringent than GDPR/CCPA



General Data Protection Regulation

- Drafted and passed by the European Union (EU)
- Toughest privacy and security law in the world
- Effective since May 25, 2018
- Imposes obligations onto organizations anywhere, so long as they target or collect data related to people in the EU.

GDPR



California Consumer Privacy Act

- Revenue > \$25m (or handles over 50,000 Personal items)
 - Receives Personal Information on CA resident
 - \$2,500 Civil Penalty per Violation
 - Controller obligations very Similar to GDPR
 - Effective Jan 1st, 2020
- 
- Processor obligations more rigorous, focus on Sale of PI, includes Households, design of Apps
 - More Transparency – Online Privacy Notices
 - Consumer has Right to Know (45 days), & to be Forgotten
 - Security is Very Important



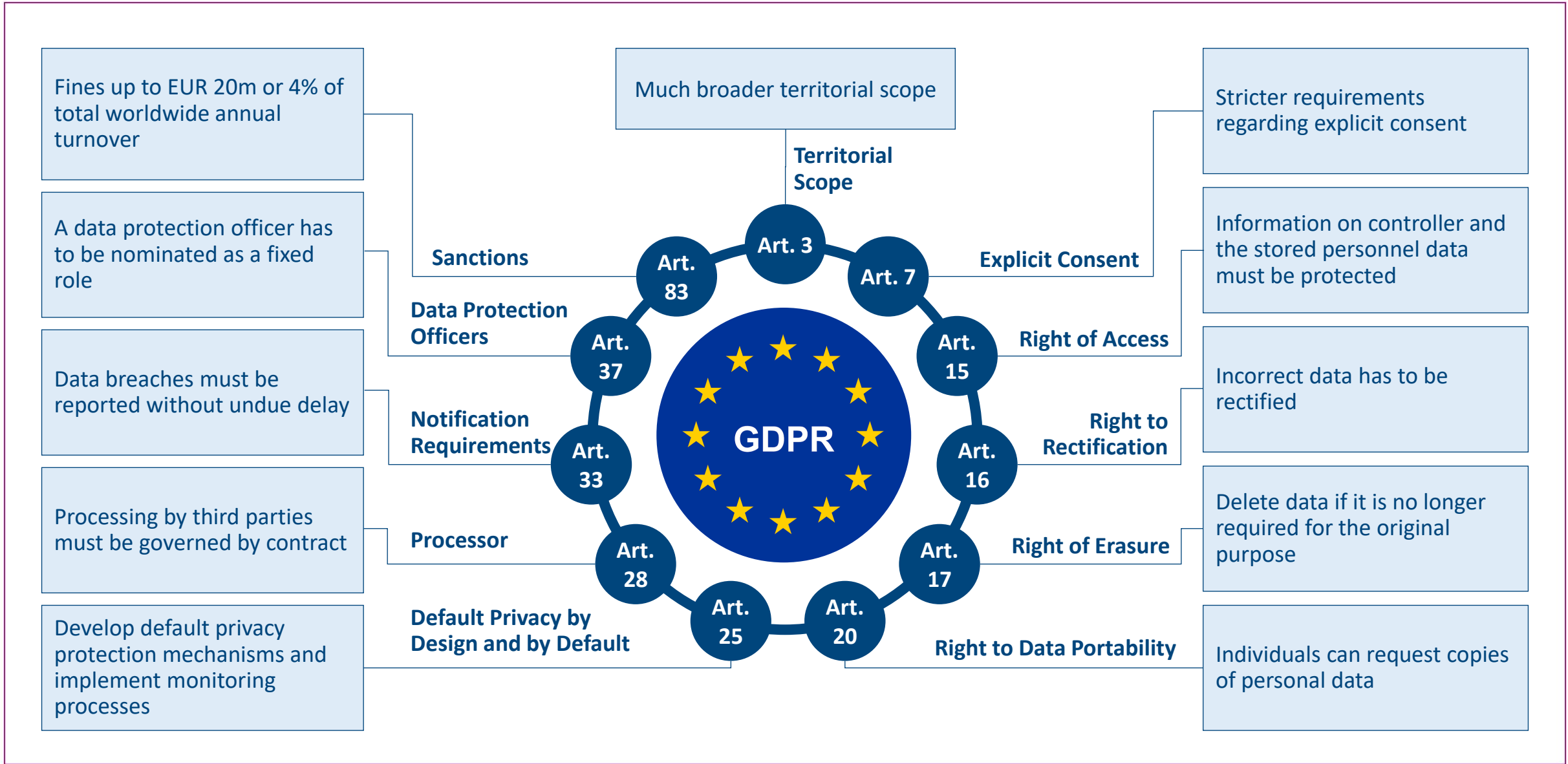
Adopted and Enforcement Date	Adopted: April 8, 2016 Enforced: May 25, 2018	Adopted: June 28, 2018 Enforced: January 1, 2020
Regulation Scope (Who)	Any entity in the world that processes personal data of an EU citizen	For profit entities doing business in California with revenues >\$25 M or processing information on 50K+ California residents
Protection Scope (Who)	Data subjects who are EU citizens	Consumers who are California residents
Protection Scope (What)	Personal data: any info relating to an identified or identifiable data subject	Information that identifies, relates to, describes, associates with, or links to customer
Security Requirements	Appropriate technical and organizational measures are mandated	None specifically named but reasonable controls implied
Fines	Up to €20 million or 4% of the annual worldwide turnover, whichever is greater	Privately: \$100 to \$50 per consumer, per incident. Civil: \$2500 - \$7500 per violation.
Right to be Forgotten / Deletion	Applies to all data collected from or about the data subject	Applies only to data collected from consumer in the last 12 months prior to the request

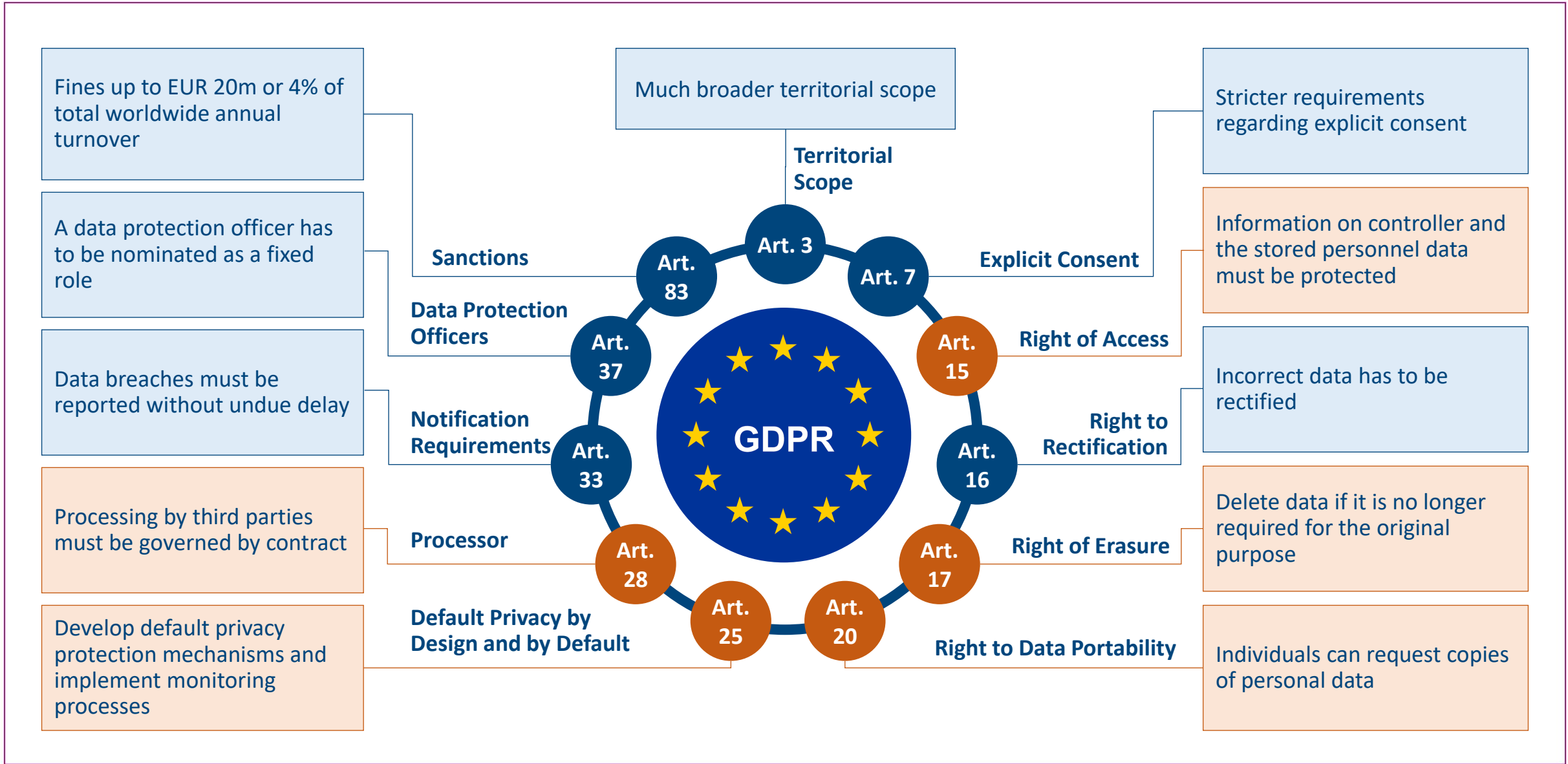


GDPR Overview

JD Edwards EnterpriseOne
and Data Privacy







GDPR Roles: Overview



Data Subject

EU resident or individual in the EU engaging with your organization that the information relates to



Data Controller (DC)

Determines how the data will be processed

Defines the how and why of personal data processing



Data Processor (DP)

Any organization that collects, processes, stores or transmits personal data (including on behalf of the data controller)

Needs to maintain an audit trail of all processing activities



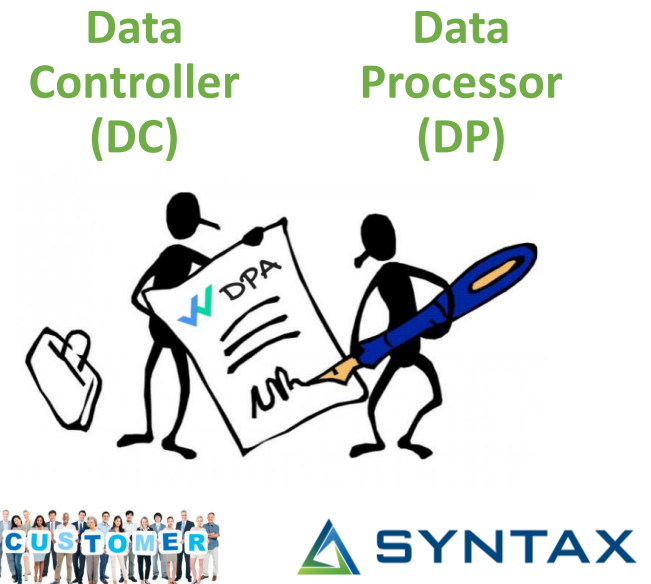
Data Controller (DC) & Data Processor (DP)

A company can have a dual role



Data Processing Agreement (DPA)

- A legally binding contract that states the rights and obligations of each party concerning the protection of personal data
- Virtually every business relies on third parties to process personal data.
- You must have a data processing agreement with all your data processors to achieve GDPR compliance
- Annoying but necessary to avoid GDPR fines

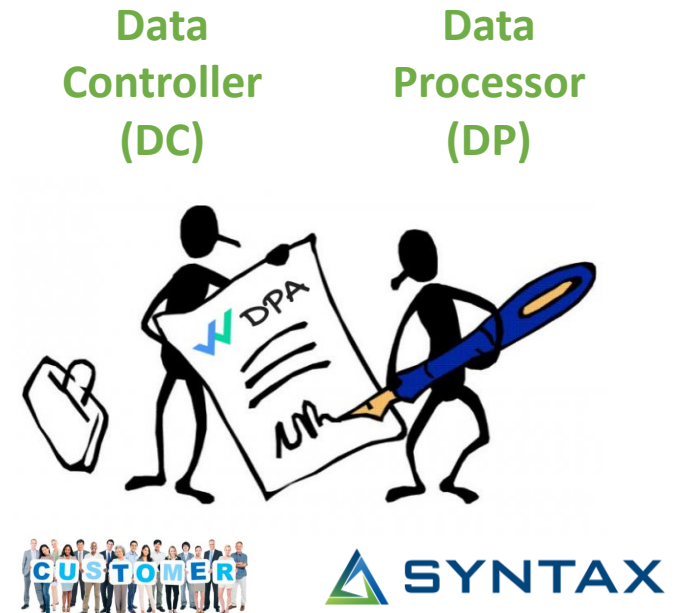


Customers require Service Providers to Sign a Data Processing Agreement Addendum

DPA Principles

Processors of personal information must comply with principles to ensure that personal information is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Kept for no longer than is necessary
6. Processed in line with the data subjects' rights
7. Secure
8. Not transferred to other countries without adequate protection

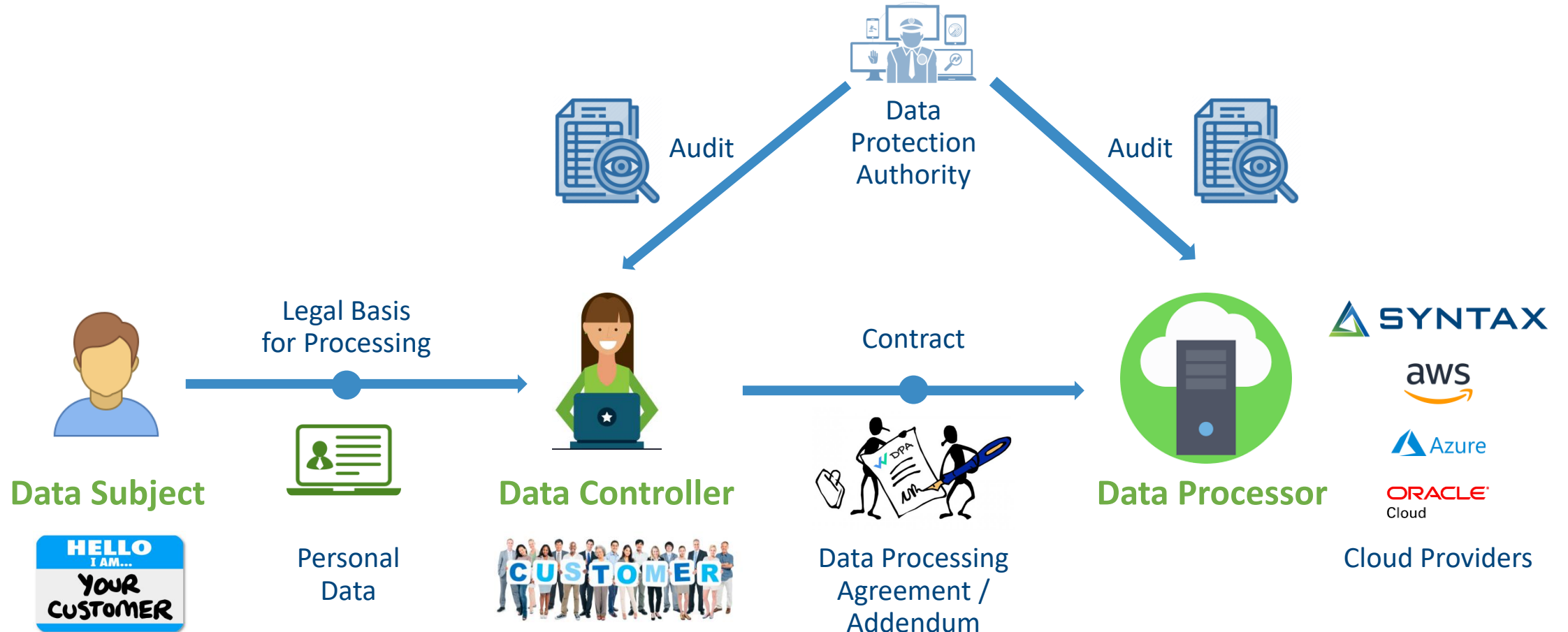


Data Protection Authority (DPAs)

- Independent public authorities that supervise, through investigative and corrective powers, the application of the data protection law.
- Provide expert advice on data protection issues and handle complaints lodged against violations of the General Data Protection Regulation and the relevant national laws.



GDPR Roles: Detailed



A close-up photograph of a computer keyboard. The central focus is a dark blue key with a white padlock icon, symbolizing security or privacy. To its right is a white key with a blue 'G' character. Below the padlock key is a white key with a blue downward-pointing arrow. The background is a soft-focus view of other keyboard keys. On the left side of the image, there are diagonal stripes in shades of pink and white.

Privacy

JD Edwards EnterpriseOne
and Data Privacy



GDPR Privacy Rights for Individuals

Personal Data

The Right to Be Informed



Individuals have a right to know who is processing their personal data.

The Right to Access



Individuals have the right to access any personal data that has been collected about them.

The Right to Rectifications



Individuals have the right to require organizations to correct inaccurate personal data.

The Right to Be Forgotten



Individuals have the right to have their personal data deleted and to prevent further collection.

The Right to Restrict Processing



Individuals have the right to require organizations to restrict the processing of specific categories of personal data.

The Right to Data Portability



Individuals have the right to require organizations to transfer personal data to a recipient of their choice.

The Right to Object



Individuals have the right to consent or withdraw consent, to the processing of their personal data.

Rights in Relation to Automated Decision Making and Profiling



Individuals have the right to opt out of the use of their personal data by automated systems.



GDPR versus CCPA Rights



- Right to be informed
- Right of access
- Right of rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object to processing
- Rights in relation to automated decision making and profiling



- Right to be request information
- Right to data portability
- Right to opt-out
- Right to access data
- Right of disclosure
- Right to deletion



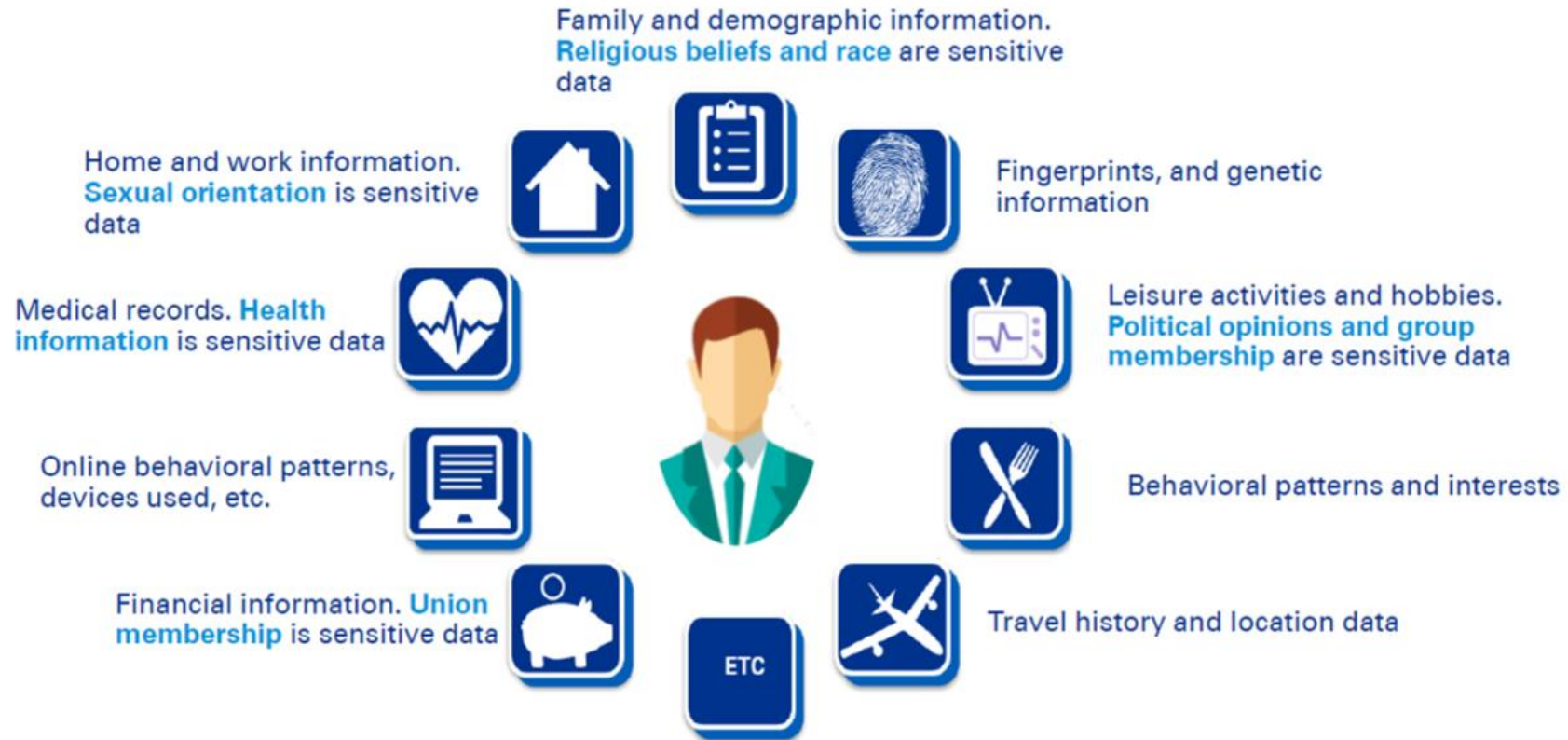
Personal Data

JD Edwards EnterpriseOne
and Data Privacy



Defining Personal Data

Personal Data is any information that can be used to identify the person.



Personal Data and ERP

- ERP systems may hold huge amounts of personal customer data and be impacted by the GDPR & CCPA
- Adopt a default culture of responsible data management
- Does the ERP system contain personal data impacted by regulation?
 - Customer needs to identify personal data
 - Privacy Policy needs to be in place
 - Service Provider requires a Privacy Policy
- GDPR now gives business only a month from the request date to present the data to the individual
 - Customization of the ERP can make achieving this timescale challenging



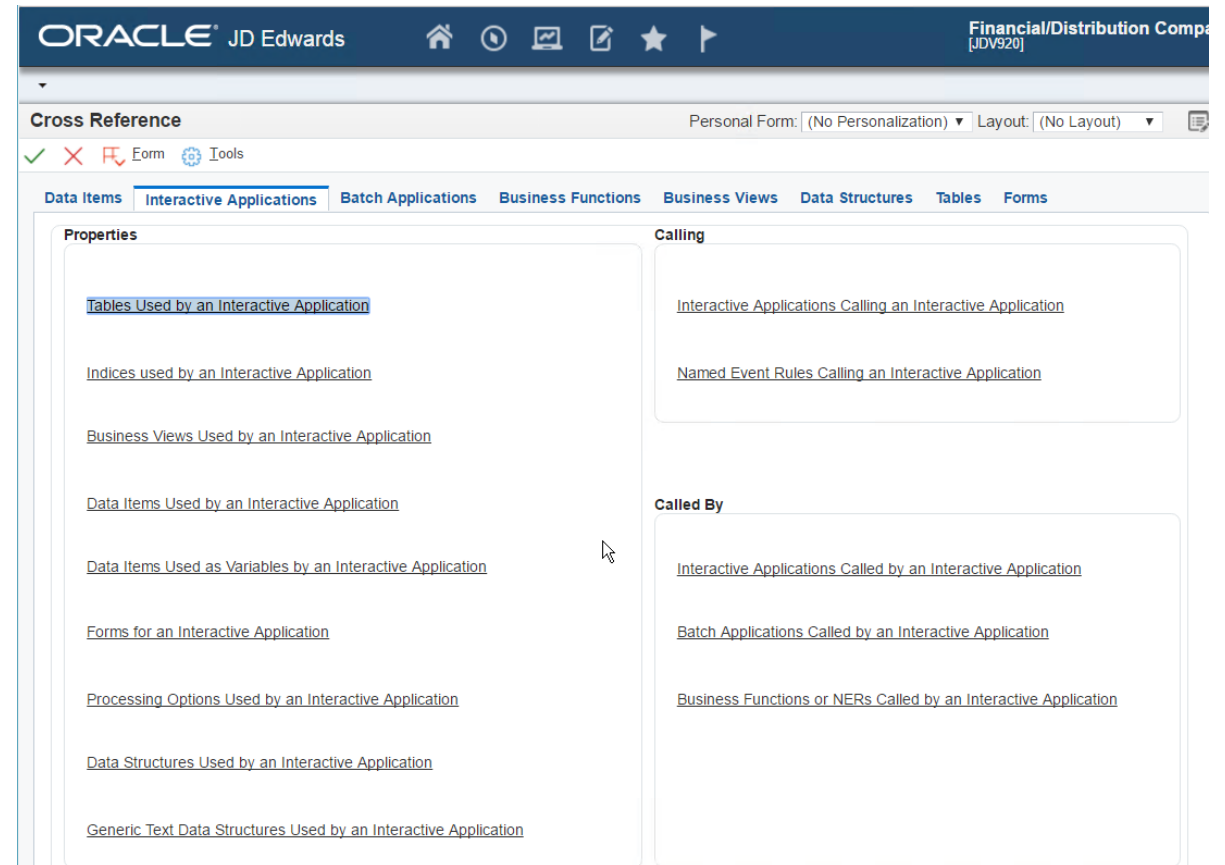
Personal Data and ERP

- Business often struggle with the 'right to be forgotten' in relation to their ERP system.
 - Businesses must be able to prove that every record of an individual's data has been completely wiped
 - Locating and erasing personal data within an ERP system is often not straight forward as personal data may be stored in several different tables across many different areas
 - Backups are a 'grey' zone
 - Potentially encrypt the data and provide the key to the customer (allow future restore)



EnterpriseOne Tools - Manual

- Cross Reference Facility
 - A tool that you can use to see complete relationship data of all the objects that exist in your E1 setup
 - Doc ID 1115756.1, 626128.1
 - P980011 and R980011
- Data Dictionary



EnterpriseOne - Personal Information

- Personal Information within JD Edwards EnterpriseOne (Doc ID 2388299.1)
- Reference which applications, tables and data dictionary items manage and store customer, supplier and employee personal information.

Personal Information within JD Edwards EnterpriseOne

March 2018

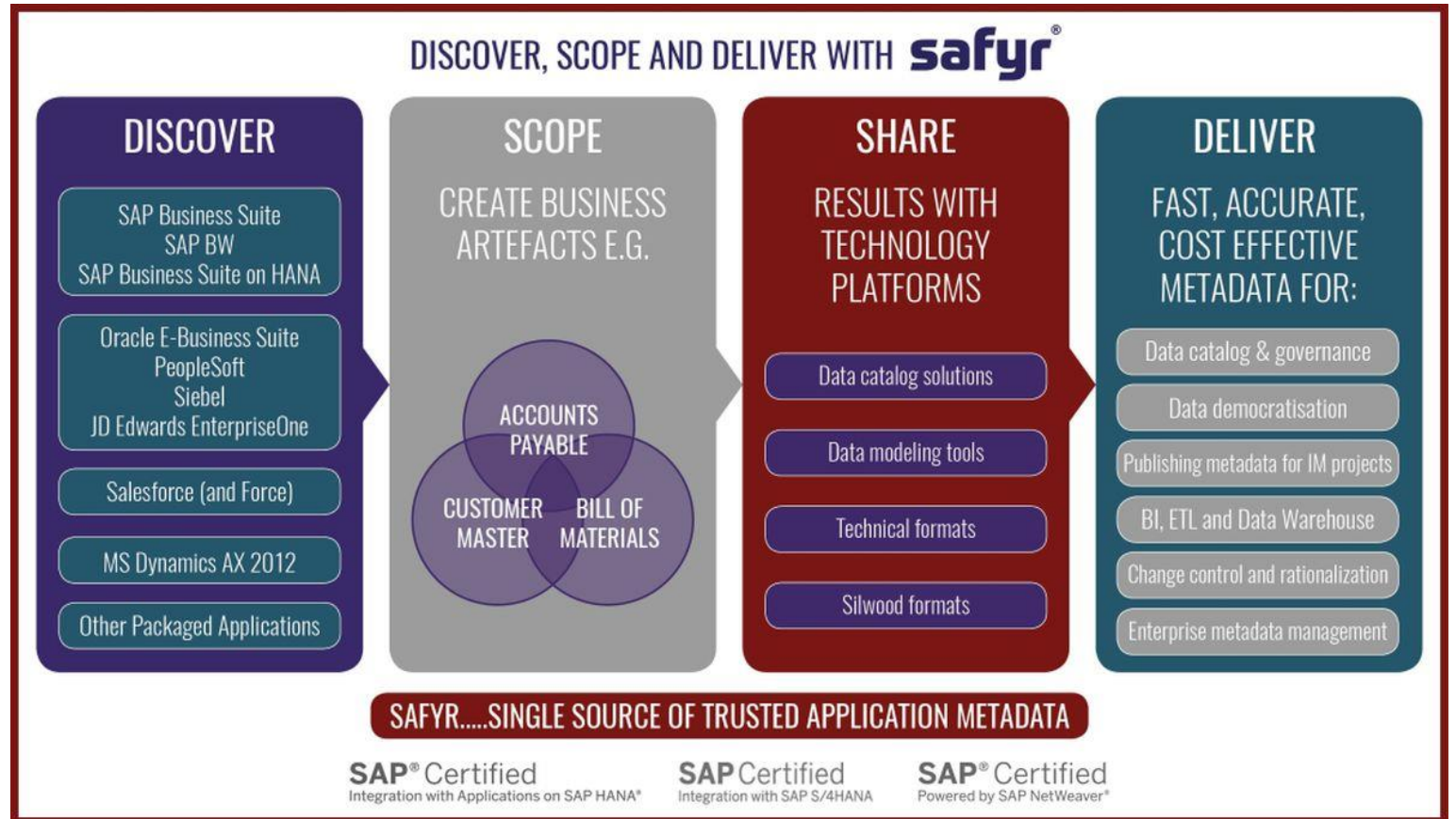
The information defined in the table below is based on JD Edwards EnterpriseOne Applications Release 9.2 as of March 2018.

Personal Information	Application Description	Application Name	Table Description	Table Name	Data Dictionary Item Description	Data Dictionary Item Name
Alien Registration Number	Employee Master	P0801	Employee Master Information	F060116	Alien Registration Number	ALRN15
Bank Account Information	Set Up Bank Accounts by Address	P0030A	Bank Transit Master	F0030	Bank Account Number – Customer	CBNK
					Transit Number – Bank	TNST
					International Bank Account Number	IBAN



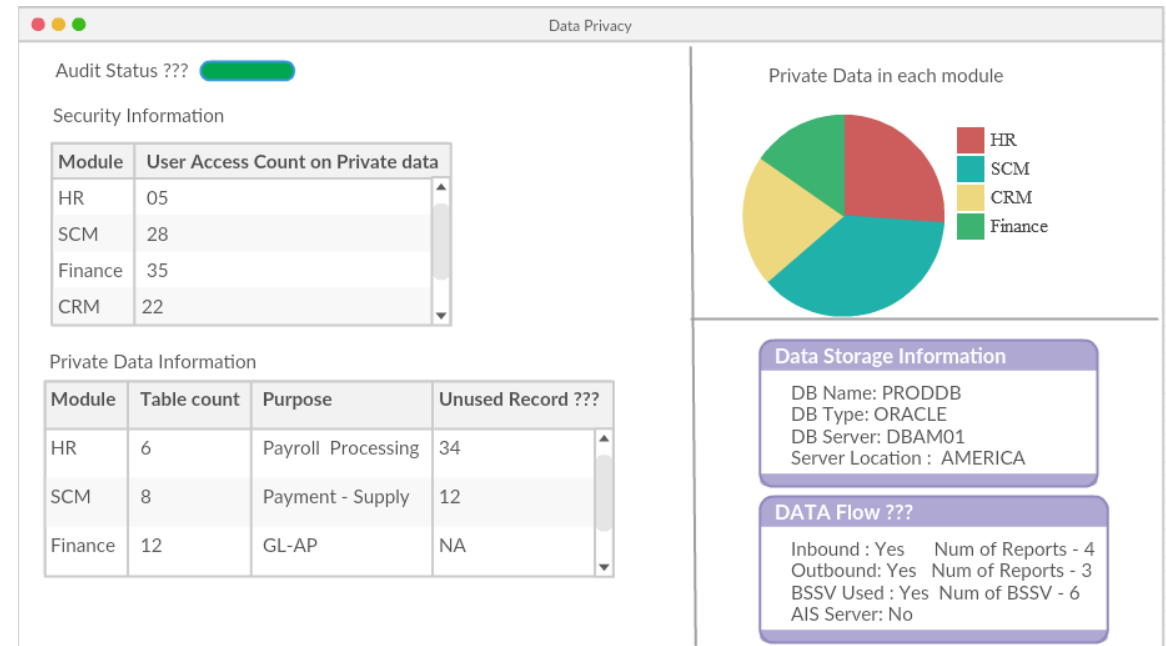
Safyr by Silwood

- Solution for finding Personal Data in ERP & CRM systems
 - <https://www.silwoodtechnology.com/products/safyr-for-oracle-jdedwards-enterpriseone/>
- JD Edwards Starter Pack for GDPR Compliance
 - <https://www.silwoodtechnology.com/jdedwards-starter-pack-for-gdpr-compliance/>



QSoftware: Data Privacy Audit - Dashboard

- **Audit Status** – Overall audit score
- **Security Information** – Users with access to the private data in each JD Edwards module.
- **Private Data Information** – Module and tables holding private data
- **Pie Chart** – Information on the volume of Private Data in each module
- **Data storage information** – Location where private data is stored
- **Data Flow** – Inbound or outbound report information used in JD Edwards



Data Protection

JD Edwards EnterpriseOne
and Data Privacy



Data Protection

- The role of a Data Protection Officer is to ensure data compliance
- Effective data security data security management is critical
- A robust security strategy and security implementation is critical:

**EnterpriseOne
Tools**

**QSoftware
Tools & Services**

**Syntax
Tools & Services**



EnterpriseOne Object Based Application Security

Object Security

- Applications Security
- Action Security
- Row Security
- Column Security
- Processing Option Security
- Tab Security
- Exit Security
- Exclusive Application Security
- External Calls
- Solution Explorer Security
- Data Browser
- Media Object
- Portal Security
- Published Business Services (BSSV)
- Data Selection Security
- Application Query Security

User Defined Object

- E1 Pages
- Data Browser
- CafeOne
- Advanced Queries
- User Overrides
- Fast Path
- Solution Explorer
- OneView Reports
- Watch Lists

Other Security

- Business Unit Security
- Password Security
- Data Privacy
- Data Change Tracker
- UDC Sharing



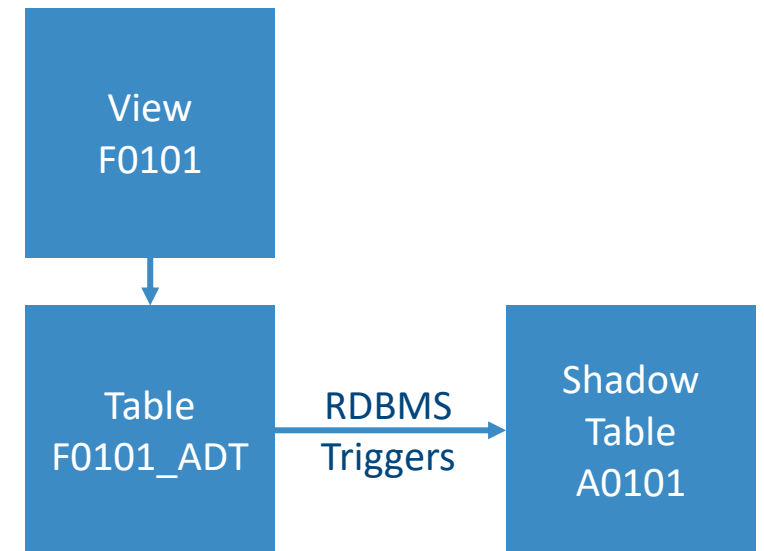
JD Edwards Tools

- Enhanced Auditing/ CFR 21 Part 11 / Data Change Tracker
 - Table level tracking
 - Triggered on one or more column changes
 - Writes entire record to the audit table
 - Triggered on Add, Change, Delete

AUDITING DISABLED



AUDITING ENABLED



EnterpriseOne Authentication

- Native Authentication Options



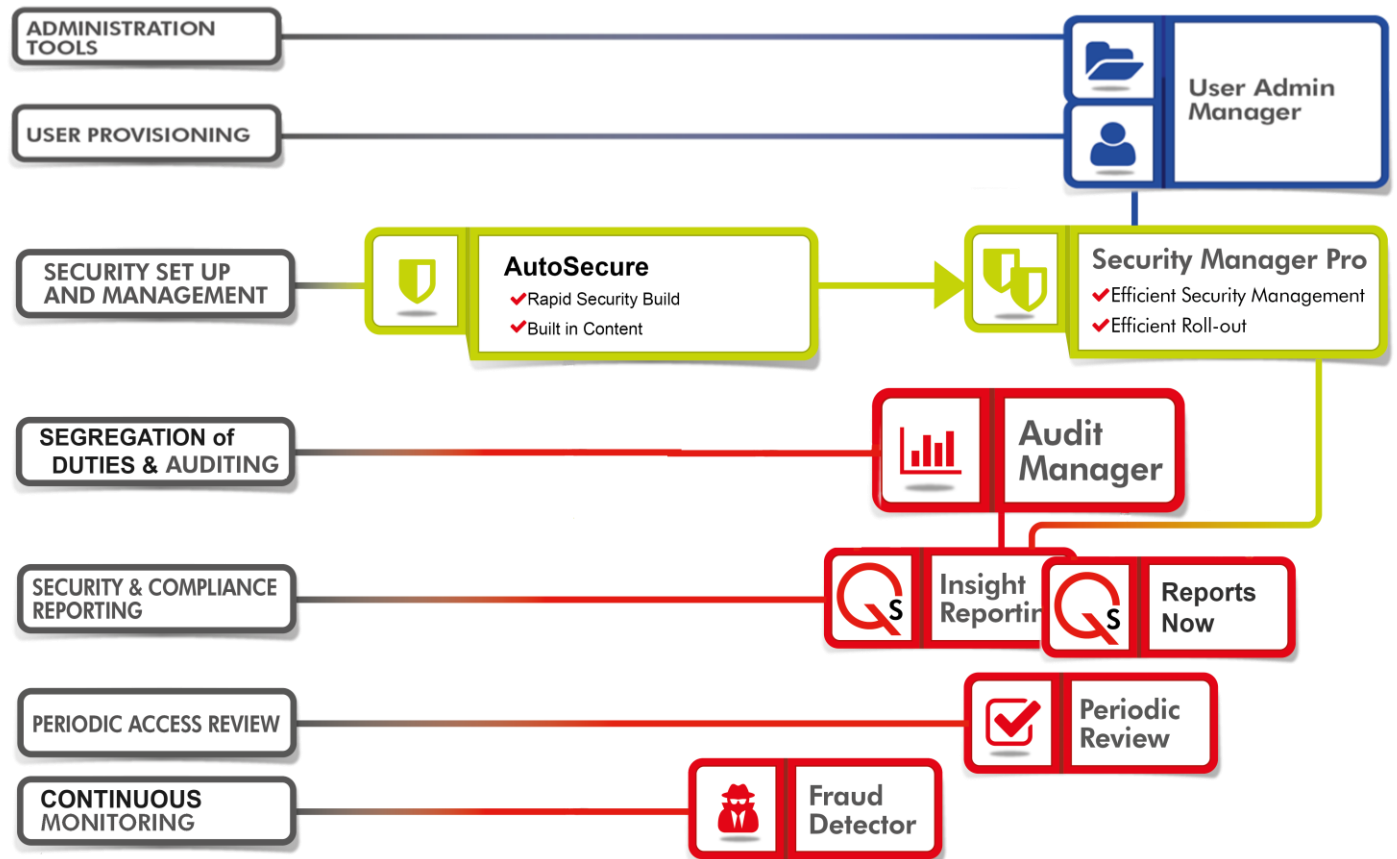
- Long Userid's and Passwords are supported with Tools 9.2+
- EnterpriseOne does not support SAML tokens
 - Oracle Access Manager (OAM) is the only official supported product for SSO configuration
- Additional authentication possible through configuration (2FA / MFA / Pre-Authentication)



Security, Compliance, & Productivity Tools



Q Software for JD Edwards EnterpriseOne simplifies and streamlines cumbersome JD Edwards tasks to reduce the workload on your valuable technical team.



The ERP Security Lifecycle



Q Cloud is an ERP Health Check

Offering and Value Prop

- Understand Segregation of Duties Issues
- Single Risk Objects – Critical Programs
- Satisfy Audit (Internal & External)
- Monitor for Potential Fraud Issues
- Compliance
- Dashboard – History & Warnings
- Remediation - Actionable



Scope and Delivery

- 4 Security Audits per Annum
- Delivered as a Managed Service
- Delivered by your MSP
- Options for License Audit
- Call to deliver results
- Optional Consultancy
- Management Dashboard - Metrics



Syntax EnCrypto

- JDE sensitive data protection with military grade encryption (AES-256)
- Column level transparent data encryption for all platforms supported by JDE
- Data is stored encrypted on the database (encrypted at rest)
- Fine grained control over who has access to decrypt what fields and columns
- Ability to encrypt specific fields defined by the user, including fields on custom tables
- On-the-fly encryption and decryption that works seamlessly across all E1 applications (forms, UBEs, business functions, data browser, UTB)



Syntax FraudID

- Transaction Monitoring
 - Suspicious activity in Payroll, Accounts Payable, Accounts Receivable, General Ledger, CNC/Security
- Transaction Pattern Analysis
 - Patterns in history files such as user, timing, frequency
- Segregation of Duties
 - Only auditors can access FraudID setup/notifications
- Robust Reporting for Auditors

Home > FraudID > Monthly Report

Monthly Report

Alert Date	Severity	Message	Disposition																								
4/2/2019 1:00:50am	High	FraudID: HR: User changed own records The following 1 employees have changed his/her own record. For complete results click here.	New																								
		<table border="1"> <thead> <tr> <th>Actor</th> <th>Date</th> <th>Machine/Application</th> <th>Employee</th> <th>Employee BU</th> </tr> </thead> <tbody> <tr> <td>SMILLS</td> <td>04/01/2019</td> <td>92ENT-EP0801CMP (Employee Basic Compensation)</td> <td>MILLS, SARAH M (58886)</td> <td>Central Branch (3)</td> </tr> </tbody> </table>	Actor	Date	Machine/Application	Employee	Employee BU	SMILLS	04/01/2019	92ENT-EP0801CMP (Employee Basic Compensation)	MILLS, SARAH M (58886)	Central Branch (3)															
Actor	Date	Machine/Application	Employee	Employee BU																							
SMILLS	04/01/2019	92ENT-EP0801CMP (Employee Basic Compensation)	MILLS, SARAH M (58886)	Central Branch (3)																							
4/2/2019 5:54:14pm	Normal	FraudID: HR: Direct deposit added or changed The following 5 direct deposit entries have been modified/created. For complete results click here.	Dismissed All ok																								
		<table border="1"> <thead> <tr> <th>Actor</th> <th>Date</th> <th>Application</th> <th>Employee</th> </tr> </thead> <tbody> <tr> <td>SMILLS</td> <td>04/02/2019</td> <td>EP055011 (Auto Deposit Instructions)</td> <td>Ellis, Jody A. (2479)</td> </tr> <tr> <td>SMILLS</td> <td>04/02/2019</td> <td>EP055011 (Auto Deposit Instructions)</td> <td>GRAWER, NICHOLE (58894)</td> </tr> <tr> <td>SMILLS</td> <td>04/02/2019</td> <td>EP055011 (Auto Deposit Instructions)</td> <td>McLind, Rod (2049)</td> </tr> <tr> <td>SMILLS</td> <td>04/02/2019</td> <td>EP055011 (Auto Deposit Instructions)</td> <td>MILLS, SARAH M (58886)</td> </tr> <tr> <td>SMILLS</td> <td>04/02/2019</td> <td>EP0801EMPA</td> <td>MILLS, SARAH M (58886)</td> </tr> </tbody> </table>	Actor	Date	Application	Employee	SMILLS	04/02/2019	EP055011 (Auto Deposit Instructions)	Ellis, Jody A. (2479)	SMILLS	04/02/2019	EP055011 (Auto Deposit Instructions)	GRAWER, NICHOLE (58894)	SMILLS	04/02/2019	EP055011 (Auto Deposit Instructions)	McLind, Rod (2049)	SMILLS	04/02/2019	EP055011 (Auto Deposit Instructions)	MILLS, SARAH M (58886)	SMILLS	04/02/2019	EP0801EMPA	MILLS, SARAH M (58886)	
Actor	Date	Application	Employee																								
SMILLS	04/02/2019	EP055011 (Auto Deposit Instructions)	Ellis, Jody A. (2479)																								
SMILLS	04/02/2019	EP055011 (Auto Deposit Instructions)	GRAWER, NICHOLE (58894)																								
SMILLS	04/02/2019	EP055011 (Auto Deposit Instructions)	McLind, Rod (2049)																								
SMILLS	04/02/2019	EP055011 (Auto Deposit Instructions)	MILLS, SARAH M (58886)																								
SMILLS	04/02/2019	EP0801EMPA	MILLS, SARAH M (58886)																								
4/2/2019 5:54:16pm	High	FraudID: HR: User changed own records The following 1 employees have changed his/her own record. For complete results click here.	New																								
		<table border="1"> <thead> <tr> <th>Actor</th> <th>Date</th> <th>Machine/Application</th> <th>Employee</th> <th>Employee BU</th> </tr> </thead> <tbody> <tr> <td>SMILLS</td> <td>04/02/2019</td> <td>92WEB-EP055011 (Auto Deposit Instructions)</td> <td>MILLS, SARAH M (58886)</td> <td>Central Branch (3)</td> </tr> </tbody> </table>	Actor	Date	Machine/Application	Employee	Employee BU	SMILLS	04/02/2019	92WEB-EP055011 (Auto Deposit Instructions)	MILLS, SARAH M (58886)	Central Branch (3)															
Actor	Date	Machine/Application	Employee	Employee BU																							
SMILLS	04/02/2019	92WEB-EP055011 (Auto Deposit Instructions)	MILLS, SARAH M (58886)	Central Branch (3)																							
4/2/2019 5:54:30pm	High	FraudID: SYS: User added to Accounts Payable Role(s) The following users have added a user to an Accounts Payable role.	New																								
		<table border="1"> <thead> <tr> <th>Actor</th> <th>Date</th> <th>Machine/Application</th> <th>Role</th> <th>User</th> </tr> </thead> <tbody> <tr> <td>JDE</td> <td>04/02/2019</td> <td>92ENT-P95921</td> <td>APMANAGER</td> <td>JDE</td> </tr> <tr> <td>SMILLS</td> <td>04/02/2019</td> <td>92ENT-P95921</td> <td>APMGRJDE</td> <td>LSTEELE</td> </tr> </tbody> </table>	Actor	Date	Machine/Application	Role	User	JDE	04/02/2019	92ENT-P95921	APMANAGER	JDE	SMILLS	04/02/2019	92ENT-P95921	APMGRJDE	LSTEELE										
Actor	Date	Machine/Application	Role	User																							
JDE	04/02/2019	92ENT-P95921	APMANAGER	JDE																							
SMILLS	04/02/2019	92ENT-P95921	APMGRJDE	LSTEELE																							

Enabled Alerts

- ✓ Hr: New Employee Created
- ✓ Hr: Direct Deposit Changed
- ✓ Hr: Direct Deposit Added
- ✓ Hr: User Changed Own Records

ed By Business Analyst

ed By System Admin

usual Pattern

ed By User Not In Payroll Role(s)

wn Deductions / Benefits Record

enerated

m Terminated To Active

r Own Deductions / Benefits Record

d For An Employee Setup For Auto Deposit

n Made To An Employee

- ✓ Ap: New Vendor Created
- ✓ Ap: Bank Account Changed
- ✓ Ap: Bank Account Created



STANDARDS

COMPLIANCE

REQUIREM

Compliance

JD Edwards EnterpriseOne
and Data Privacy



Compliance

- Compliance is mostly contractual
- Scope for Concern
 - 72 Controller concerns
 - 43 Processor concerns
- Onus is on the customer for compliance
- Security services is a small component ~15%

SCOPE FOR CONCERN			
Sub Category	Question	Controller	Processor
Data Protection Officers (DPOs)	Do you need to appoint a DPO?	Y	
	If a DPO is not required, consider whether one should be appointed.	Y	
	Where a DPO is appointed are escalation and reporting lines in place?	Y	
Demonstrating compliance (record keeping)	How many employees does the company have?	Y	
	Is sensitive personal data processed?	Y	
	Are the legal grounds for processing personal data recorded?	Y	
Data Protection Impact Assessments (DPIAs)	Do you have a process for identifying the need for and conducting (and documenting) DPIAs?	Y	
	Do you undertake and record prior diligence of service providers?	Y	
	Are all the stipulated terms included in processor contracts?	Y	
Data processor contracts	Are there controller/processor contracts containing all the stipulated terms?	Y	
Other processor obligations			
Contracts with controllers	Are there controller/processor contracts in place containing the stipulated terms?		Y
Use of sub-processors	Is there written authorization for existing sub-processing arrangements?		Y
	Is there written authorization for proposed sub-processing?		Y
	Has specific or general authorization been provided?		Y
	If general authorization, is there a process for informing the controller of any intended changes to		Y



Compliance Checklist

1

Awareness and Communication

Ensure your employees understand GDPR and communicate with service and staff about why you are collecting the data.



2

Analysis of Personal Data

Analyze a list of all sensitive data you store and process



3

Review Procedures

Have a suitable privacy policy in place and review it regularly



4

Access Rights

List what access rights should be granted and how changes should be handled



5

Customer Consent

Ensure your customers consent to you processing their data



6

Data Breaches

Implement a procedure for handling data breaches



7

Impact assessments

Carry out a data protection impact assessment



8

Data Protection Officers (DPO's)

Determine whether you need a Data Protection Officer (DPO)



A close-up photograph of several hands holding pens and writing in notebooks, set against a blurred background of papers and office equipment. The image is partially obscured by a large, light pink geometric shape on the left side of the slide.

Summary

JD Edwards EnterpriseOne
and Data Privacy



Summary



Ensure that your organization is aware of data privacy legislation.



Determine whether your organization is subject to data privacy legislation.



Work with a vendor who have a firm understanding of privacy legislation (CCPA, GDPR, PIPEDA).



Look for vendors that can offer a complete range of tools and services to ensure data compliance.



An updated Data Protection Agreement and effective data security data security management are critical.





Q&A

cdawes@syntax.com
mikew@qsoftware.com

Session ID:

Quest2020-114220

*Remember to provide your
session feedback in the app!*



Quest Forum Digital Event



Thank You

JD Edwards EnterpriseOne
and Data Privacy



Quest Forum Digital Event Continues!

Cloud Week

Wednesday, May 27 - Friday, May 29

PeopleSoft Week

Monday, June 1 - Thursday, June 4

Professional Development & Emerging Technology Day

Friday, June 5

JD Edwards Week

Monday, June 8 - Thursday, June 11

Training & Workshops Day

Friday, June 12

Database & Technology Week

Monday, June 15 - Thursday, June 18

REGISTER TODAY!

Syntax

Overview



Syntax Overview

SCHOLASTIC

CBS

Ansell

petco

RH
RESTORATION HARDWARE

Milgard
WINDOWS & DOORS

Honeywell
Intelligent

ATRIUM
INNOVATIONS

SOULCYCLE

KIND
HEALTHY SNACKS

HAVI

Domtar

45+

Years
in Technology

1.2K

Employees
Globally

40

Years Supporting
Oracle & SAP ERP

25

Years of Cloud
Managed Services

MOTOR
HARLEY-DAVIDSON
CYCLES

Lindt

LATICRETE

LEDCOR
GROUP

ART.
COM

Fidelity &
Guaranty Life

Tt
TETRA TECH

CR
Consumer
Reports

e-Cycle
Recycle. Recover. Protect.

ANALOG
DEVICES

R
T
R

LOOMIS

THULE
SWEDEN

Harper
Collins

GII

W
chefsWAREHOUSE

Syntax Global Capabilities



- Remote Technical Managed Services
- Other Oracle/SAP and 3rd-Party Apps



Oracle ERP Cloud Solutions

Hybrid/Public Cloud Solutions



Application Managed Services

- Enterprise Application Managed Services
- Enterprise Application Development & Enhancements
- SOA and Middleware Development
- Business Intelligence
- Enterprise Planning and Advisory

Associated Technologies



Consulting Solutions

- License Sales
- Implementations & Upgrades
- Project Management
- Technical Support
- Functional Support
- Training
- Custom Programming

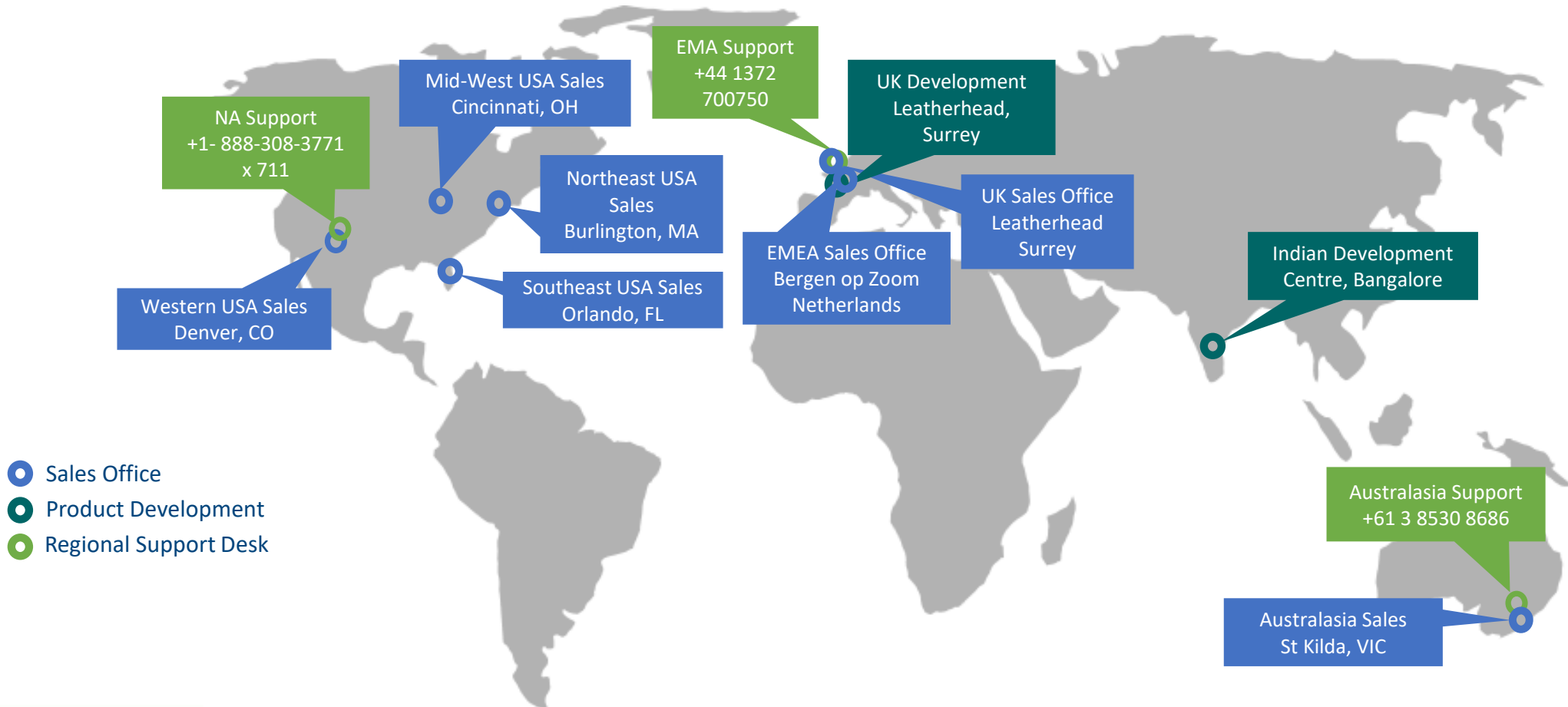
- Interfaces
- Integrations
- Replication Technologies

Q Software

Overview



Q Software - A Worldwide Business



Q Software – By the Numbers

- **20+** Years in JDE Audit & Security Management
- **300+** Customers
- **95%** Customer Retention Rate
- **350+** Audits (100+ on QC)
- **100+** Person Years Development

