JD Edwards EnterpriseOne and the Implications of GDPR

Name: Colin Dawes
Title: Chief Solution Architect
Company: Syntax
Email: cdawes@syntax.com

Name: Mike Ward
Title: President
Company: QSoftware
Email: mikeq@qsoftware.com

Session ID#: 102230
Tuesday August 20, 2019
2:00 pm – 3:00 pm MST

#JDEINFOCUS
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
Company Overviews
Syntax Overview

45+ Years in Technology
1.2K+ Employees globally
40 Years Supporting Oracle & SAP ERP
25 Years of Cloud Managed Services
Syntax Global Capabilities

Office and Data Center Locations

Account Management & Technical Support

Phoenix, AZ
Montreal, QC
Edison, NJ
Germany
China
- Remote Technical Managed Services
- Other Oracle/SAP and 3rd-Party Apps
- Enterprise Application Managed Services
- Enterprise Application Development & Enhancements
- SOA and Middleware Development
- Business Intelligence
- Enterprise Planning and Advisory

ERP Cloud Solutions

Hybrid/Public Cloud Solutions

Associated Technologies

Consulting Solutions

Syntax Technologies

- License Sales
- Implementations & Upgrades
- Project Management

- Technical Support
- Functional Support
- Training
- Custom Programming

- Interfaces
- Integrations
- Replication Technologies
Q Software – By the Numbers

• 20+ Years in JDE Audit & Security Management
• 300 Customers
• 96% Customer Retention Rate
• 200+ Audits
• 100+ Person Years Development
GDPR Overview
<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
<th>Effective</th>
<th>Applicable To</th>
<th>Applies To</th>
</tr>
</thead>
<tbody>
<tr>
<td>GDPR</td>
<td>General Data Protection Regulation</td>
<td>May 28, 2018</td>
<td>All individuals within the European Union (EU) and the European Economic Area (EEA)</td>
<td>Anyone who processes the personal data of EU individuals</td>
</tr>
<tr>
<td>CCPA</td>
<td>California Consumer Privacy Act of 2018</td>
<td>Jan 1, 2020</td>
<td>California Residents</td>
<td>Anyone who processes the personal data of California residents</td>
</tr>
<tr>
<td>PIPEDA</td>
<td>The Personal Information Protection and Electronic Documents Act</td>
<td>April 13, 2000</td>
<td>All businesses that operate in Canada</td>
<td>All businesses that handle personal information</td>
</tr>
</tbody>
</table>
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
California Consumer Privacy Act (CCPA)

- Compliance Deadline January 1st 2020
- 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
- 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
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.
Much broader territorial scope

Fines up to EUR 20m or 4% of total worldwide annual turnover

A data protection officer has to be nominated as a fixed role

Data breaches must be reported without undue delay

Processing by third parties must be governed by contract

Develop default privacy protection mechanisms and implement monitoring processes

Stricter requirements regarding explicit consent

Information on controller and the stored personnel data must be protected

Incorrect data has to be rectified

Delete data if it is no longer required for the original purpose

Individuals can request copies of personal data

Sanctions

Explicit consent

Right of access

Right to rectification

Right of erasure

Right to data portability

Default privacy by design and by default

Territorial scope

Data protection officers

Notification requirements

Processor

Art. 3

Art. 83

Art. 37

Art. 33

Art. 28

Art. 25

Art. 20

Art. 15

Art. 16

Art. 17

Art. 7

Art. 3

Art. 20

Art. 3

Art. 7

Art. 3

Art. 28

Art. 25

Art. 17

Art. 16

Art. 15

Art. 17

Art. 16

Art. 15

Art. 7

Art. 3

Art. 20

Art. 3

Art. 7

Art. 3

Art. 20

Art. 3

Art. 7

Art. 3

Art. 20

Art. 3
Much broader territorial scope

Fines up to EUR 20m or 4% of total worldwide annual turnover

A data protection officer has to be nominated as a fixed role

Data breaches must be reported without undue delay

Processing by third parties must be governed by contract

Develop default privacy protection mechanisms and implement monitoring processes

Sanctions

Territorial scope

Explicit consent

Art. 3

Art. 7

Art. 15

Art. 16

Art. 17

Art. 20

Art. 25

Art. 28

Art. 33

Art. 37

Art. 83

Data protection officers

Notification requirements

Processor

Default privacy by design and by default

Right of access

Right to rectification

Correct data has to be rectified

Delete data if it is no longer required for the original purpose

Individuals can request copies of personal data

Stricter requirements regarding explicit consent

Information on controller and the stored personnel data must be protected

Incorrect data has to be rectified

Delete data if it is no longer required for the original purpose

Individuals can request copies of personal data

#JDEINFOCUS
GDPR Roles

Data Control,
Data Processing,
& Contracts
Much broader territorial scope

- Fines up to EUR 20m or 4% of total worldwide annual turnover
- A data protection officer has to be nominated as a fixed role
- Data breaches must be reported without undue delay
- Processing by third parties must be governed by contract
- Develop default privacy protection mechanisms and implement monitoring processes

GDPR

- Art. 3: Explicit consent
- Art. 7: Right of access
- Art. 15: Right to rectification
- Art. 16: Right of erasure
- Art. 17: Right of erasure
- Art. 20: Right to data portability
- Art. 25: Right to data portability
- Art. 28: Processor
- Art. 37: Data protection officers
- Art. 33: Notification requirements
- Art. 83: Sanctions

Strict requirements regarding explicit consent
- Information on controller and the stored personnel data must be protected
- Incorrect data has to be rectified
- Delete data if it is no longer required for the original purpose
- Individuals can request copies of personal data

Sanctions

- Art. 83
- Art. 37
- Art. 33
- Art. 28
- Art. 25
- Art. 20
- Art. 17
- Art. 16
- Art. 15
- Art. 14
- Art. 13
- Art. 12
- Art. 11
- Art. 10
- Art. 9
- Art. 8
- Art. 7
- Art. 6
- Art. 5
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

- Data Subject
- Data Controller
- Data Processor

Legal Basis for Processing

Personal Data

Contract

Audit

Data Protection Authority

Data Processing Agreement / Addendum

Cloud Providers

Cloud Providers
Privacy and Personal Data
Much broader territorial scope

- Fines up to EUR 20m or 4% of total worldwide annual turnover
- A data protection officer must be nominated as a fixed role
- Data breaches must be reported without undue delay
- Processing by third parties must be governed by contract
- Develop default privacy protection mechanisms and implement monitoring processes

GDPR

- Explicit consent
- Right of access
- Right to rectification
- Right of erasure
- Right to data portability
- Default privacy by design and by default
- Notification requirements
- Sanctions

Art. 3  Art. 7  Art. 15  Art. 16  Art. 17  Art. 20  Art. 25  Art. 28  Art. 33  Art. 37

Stricter requirements regarding explicit consent
- Information on controller and the stored personnel data must be protected
- Incorrect data has to be rectified
- Delete data if it is no longer required for the original purpose
- Individuals can request copies of personal data

#JDEINFOCUS
**GDPR Expands Privacy Rights to Individuals Personal Data**

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>The Right to Be Informed</strong></td>
<td>Individuals have a right to know who is processing their personal data</td>
</tr>
<tr>
<td><strong>The Right to Access</strong></td>
<td>Individuals have the right to access any personal data that has been collected about them</td>
</tr>
<tr>
<td><strong>The Right to Rectifications</strong></td>
<td>Individuals have the right to require organizations to correct inaccurate personal data</td>
</tr>
<tr>
<td><strong>The Right to Be Forgotten</strong></td>
<td>Individuals have the right to have their personal data deleted and to prevent further collection</td>
</tr>
<tr>
<td><strong>The Right to Restrict Processing</strong></td>
<td>Individuals have the right to require organizations to restrict the processing of specific categories of personal data</td>
</tr>
<tr>
<td><strong>The Right to Data Portability</strong></td>
<td>Individuals have the right to require organizations to transfer personal data to a recipient of their choice</td>
</tr>
<tr>
<td><strong>The Right to Object</strong></td>
<td>Individuals have the right to consent, or withdraw consent, to the processing of their personal data</td>
</tr>
<tr>
<td><strong>Rights in Relation to Automated Decision Making and Profiling</strong></td>
<td>Individuals have the right to opt out of the use of their personal data by automated systems, such as artificial intelligence</td>
</tr>
</tbody>
</table>
Defining Personal Data

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

- Family and demographic information. Religious beliefs and race are sensitive data.
- Home and work information. Sexual orientation is sensitive data.
- Medical records. Health information is sensitive data.
- Online behavioral patterns, devices used, etc.
- Financial information. Union membership is sensitive data.
- Fingerprint, and genetic information.
- Leisure activities and hobbies. Political opinions and group membership are sensitive data.
- Behavioral patterns and interests.
- Travel history and location data.
- ETC.
Personal Data and ERP

• ERP systems may hold huge amounts of personal customer data and be impacted by the GDPR
• 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 straightforward 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.

<table>
<thead>
<tr>
<th>Personal Information</th>
<th>Application Description</th>
<th>Application Name</th>
<th>Table Description</th>
<th>Table Name</th>
<th>Data Dictionary Item Description</th>
<th>Data Dictionary Item Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>Alien Registration Number</td>
<td>Employee Master</td>
<td>PO001</td>
<td>Employee Master Information</td>
<td>PO00116</td>
<td>Alien Registration Number</td>
<td>ALRN15</td>
</tr>
<tr>
<td>Bank Account Information</td>
<td>Set Up Bank Accounts by Address</td>
<td>PO0030A</td>
<td>Bank Transit Master</td>
<td>F0030</td>
<td>Bank Account Number – Customer</td>
<td>CBIN</td>
</tr>
</tbody>
</table>

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

- Solution for finding Personal Data in ERP & CRM systems

- JD Edwards Starter Pack for GDPR Compliance
QSoftware: Data Privacy Audit - Dashboard
QSoftware: Data Privacy Audit - Dashboard

The Initial Dashboard page will have the below categories:

- **Audit Status** – Overall score for the Data privacy audit.
- **Security Information** – Shows how many users have access to the private data in each JDE module.
- **Private Data Information** – Shows the module and its table, holding private data, its purpose in the module and count of unused private records.
- **Pie Chart** – Gives clear information on the amount of Private Data in each JDE module
- **Data storage information** – Provides information on where the data is stored (Database information).
- **Data Flow** – This shows the information on if any inbound or outbound report was used in JDE, its count, and Usage of BSSV and its count.

Clicking on each of the sections shall get the detailed information in a popup.
Data Protection
Much broader territorial scope

Fines up to EUR 20m or 4% of total worldwide annual turnover

A data protection officer has to be nominated as a fixed role

Data breaches must be reported without undue delay

Processing by third parties must be governed by contract

Develop default privacy protection mechanisms and implement monitoring processes

Sanctions

Territorial scope

Explicit consent

Data protection officers

Notification requirements

Processor

Default privacy by design and by default

Right of access

Right to rectification

Right of erasure

Right to data portability

Art. 3

Art. 7

Art. 15

Art. 16

Art. 17

Art. 25

Art. 20

Art. 28

Art. 33

Art. 37

Art. 83

Incorrect data has to be rectified

Delete data if it is no longer required for the original purpose

Individuals can request copies of personal data

Stricter requirements regarding explicit consent

Information on controller and the stored personnel data must be protected
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 Security Tools

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
EnterpriseOne Security Tools

User Defined Object Security

• EnterpriseOne Pages
• EnterpriseOne Data Browser
• EnterpriseOne CafeOne
• EnterpriseOne Advanced Queries
• EnterpriseOne User Overrides
• EnterpriseOne Fast Path
• EnterpriseOne Solution Explorer
• EnterpriseOne OneView Reports
• EnterpriseOne 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

| Table F0101 |

Auditing Enabled

<table>
<thead>
<tr>
<th>View F0101</th>
</tr>
</thead>
</table>

| Table F0101_AD T |

| RDBMS Triggers |

| Shadow Table A0101 |
EnterpriseOne Authentication

• Authentication

1. ORACLE®
   JD EDWARDS

2. LDAP
   Windows Server
   Active Directory

3. Windows Native Authentication (SSO)

# JDEINFOCUS
QSoftware Integrated Toolset

- Limit Access to Essential Users
- Segregation of Duties (stop thieves)
- Approvals on Provisioning
- Monitor Critical Tables (stop data theft)
QSoftware Tools

• QCloud Audit As A Service
  • Existing audit processes are manual
    • IT staff create reports
    • SQL/manual
    • Cobbled together spreadsheets
    • Auditors Review & Question (& loop)
  • Tools
    • Specialist On-Prem (Audit Manager)
    • Expensive & Very Complex (Oracle GRC/AACG)
  • QCloud Automates
    • Customer Log In
    • Request, Review
    • Download Report
QSoftware: Module Usage

• Input Oracle License
• Request Audit – No technical requirements
• Report will show
  • Usage by Module
  • Non-Compliance Modules
  • Custom Modules
• Combi – SA & LA - Look at Users/Roles to Determine Usage & Remove unnecessary access
QSoftware

plan & remediate

QCloud

Oracle licensing

audit on demand

data privacy

segregation of duties & fraud control

history & drill down
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

• Closely monitors JDE production data
• Perform pattern analysis to identify unusual transactions
• Proactively detects and alerts for suspicious JDE transactions
• Over 30 built-in rules for AP, HR, and CNC
• Alerts auditors and controllers in real-time
Compliance

• GDPR Compliance is mostly contractual

• GDPR Scope for Concern
  • 72 Controller concerns
  • 43 Processor concerns

• Onus is on the customer for compliance

• Security services is a small component ~15%
GDPR 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).
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 management are critical
Thank You
Please complete a session evaluation

Session ID: 102230

Contact Info:
Colin Dawes
cdawes@syntax.com

Contact Info:
Mike Ward
mikew@qsoftware.com