European General Data Protection Regulation is looming in 2018!
How to master the challenge of Data Protection and Security?

Considerations for Your Progress® OpenEdge® Application

Jarmo Nieminen, Laurent Kiefer and Stefan Bolte
EMEA Solution Engineer Team
17. November 2017
DISCLAIMER:

This presentation is intended to provide general information regarding GDPR, as well as highlight certain features of Progress® OpenEdge®. It is not intended to be, and does not constitute, legal advice. If you have specific questions regarding GDPR or how it applies to your organization, please consult your attorney or privacy professional.
AGENDA

- GDPR
  - What is GDPR?
  - Why GDPR?
  - Who is Impacted?

- OpenEdge Features to consider
  - How to Assess Your OpenEdge App for GDPR Preparation?
  - OpenEdge features that help to craft your strategy

- Where Can You Get More Information?
What and Why GDPR?
General Data Protection Regulation (GDPR)
(Regulation (EU) 2016/679)

A regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU).

https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
GDPR Timeline

1995
EU Data Protection Directive

1998
Data Protection Act

June 2015
European Council approves EU General Data Protection Regulation draft

April 27, 2016
GDPR adopted

May 25, 2018
GDPR officially goes into effect
Market Factors Setting the Stage

- Digital Acceleration
- Deluge of Data
- Device Explosion
- Malicious Security Acts
Major Aspects of GDPR

• Territorial Scope, Fines

• Expanded Rights of Individuals
  • Access/Rectification
  • Portability
  • Erasure

• Obligations of Data Controllers
  • Privacy by Design, Privacy by Default
  • Data Protection Impact Assessments
  • Record of Processing
  • Breach Notification

• Obligations of Data Processors
  • Processing based on instruction of Data Controller
  • Appropriate technical and organizational measures
Who Does It Impact?
Companies Worldwide are Concerned about the Impact of GDPR

- **86%** Concerned that if they do not comply, it will have a major negative impact on their business
- **42%** Admitted they have no mechanism for determining which data should be saved or deleted
- **32%** Fear they do not have necessary technology to manage data effectively, limiting their ability to adhere to GDPR
- **18%** Worried noncompliance could put them out of business

Misnomers about Who is Impacted

**Only impacts companies located within the EU**

**Truth:**
This will impact entities that collect, use or store European personal data both inside and outside of Europe.

**Small businesses are exempt from GDPR**

**Truth:**
Exemptions are based on the comparative risk that they pose to EU citizens, not determined by company size.

If you conduct business within the EU, or you collect, process and/or store personal data of EU citizens, you should assess your potential risk of not adhering to GDPR requirements.
“By failing to prepare, you are preparing to fail.”

— Benjamin Franklin
Assess Your Application
Seven Key Considerations

- Do you collect, process and store personal data?
- How is personal data secured in your application, including when it is in transit and at rest?
- What technology do you have in place to ensure proper authentication and authorization access to personal data, both internally and externally?
- How do you track manipulation of personal data?
- Can you ensure that personal data is handled consistently across systems?
- Do you support companies that collect, store and process personal data?
- How is handling personal data automated and governed by rules?
Three Groups of Provisions

- **Safeguard**: Protect personal data by e.g. encryption, implement a strong password policy.
- **Govern**: Define handling and maintenance of personal data to assure compliance, by e.g. purge rules, limiting access to data base on the role in a process.
- **Monitor and Report**: Assess your provisions. Eliminate areas of non-compliance, report intrusions and theft of personal data.
Address the Challenge

We get support by a smart Team!

They know the questions to ask

They got the smart ideas

They have got the smart Tools.
How does OpenEdge help me to flesh out the strategy?

- Data Encryption
- Disaster Recovery
- Auditing
- Effective Resource Management
- Cloud Scale and Manage
- Application Server
- Identity Management
- Business Process Management
- Business Rules Management
- Data Accuracy

Available in the Advanced Enterprise Edition
Protecting & Accessing the Data
Seven Key Considerations

- Do you collect, process and store personal data?
- How is personal data secured in your application, including when it is in transit and at rest?
- What technology do you have in place to ensure proper authentication and authorization access to personal data, both internally and externally?
- How do you track manipulation of personal data?
- Can you ensure that personal data is handled consistently across systems?
- Do you support companies that collect, store and process personal data?
- How is handling personal data automated and governed by rules?
Protecting the Data

- **Progress Application Server for OpenEdge**: Next gen application server to modernize applications. Provides industry standard security and authentication and authorization control via Tomcat and Spring Security.

- **OpenEdge Transparent Data Encryption (TDE)**: Protects personal data by encrypting all or part of your database while at rest. Verification with auditors that you have taken proper measures to protect data.

- **OpenEdge Authentication Gateway**: Centralizes authentication and authorization service for database access, providing trusted identity management.

- **Newly Available! OpenEdge 11.7**: Provides security updates to the entire platform helping ensure your application is leveraging the latest security standards and technology.
How do I ..?

- Protect personal data against unauthorized reading …
- if an intruder copies the database?
- if I cannot find some backup media?
- if a disk gets replaced and the old one is still accessible?
- if an external consultant needs to maintain the system and I need to prove he cannot read that data?
## Transparent Data Encryption

<table>
<thead>
<tr>
<th>Ease of Maintenance</th>
<th>High-Performance</th>
<th>Cost-Effective</th>
</tr>
</thead>
<tbody>
<tr>
<td>Complete “in the box” solution that requires no changes to your application, procedures or Database Administrator (DBA) management processes.</td>
<td>Less than 2% performance degradation while encrypting/decrypting.</td>
<td>Configure encryption for only those database objects requiring it, providing protection at the lowest possible cost.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Protect What Needs Protecting</th>
<th>Managed DB Access</th>
<th>Seamless Protection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encrypt everything (or a subset) in your database protecting your sensitive information from unauthorized access while on-disk, backup, and binary dumps.</td>
<td>Includes both policy tools and a secure encryption key store kept separate from the database to manage access to the encrypted database.</td>
<td>Leverages the authentication, authorization, and auditing functionality inherent in OpenEdge and additional ABL security features to provide seamless protection of your data.</td>
</tr>
</tbody>
</table>
Encrypting Database Objects

- Full Protection throughout the Data Lifecycle
  - On disk, backups, binary dumps
- Industry standard cipher algorithms
  - AES, DES, triple DES, etc.
- It is driven by Policies and Security Manager can change the encryption regularly
- Cannot breach by Code (ABL or SQL)
Unencrypted DB Extent

Encrypted DB Extent
Contribution of TDE to your solution

- strong encryption based on acknowledged industry standards protect against any unauthorized reading by direct access to data files
- Helps certifying that protection measures are meeting internal policies and external requirement
- Can be enabled for your application without coding or changing your application code.

OpenEdge Transparent Data Encryption (TDE)

Protects personal data by encrypting all or part of your database while at rest. Verification with auditors that you have taken proper measures to protect data.
How do I ..?

- manage access to personal data by the application?
- make sure that access is governed by identity and role?
- establish a central point of authorization maintenance?
- track user access and potential intrusion events?
- inhibit any other way of accessing database data?
OpenEdge Authentication Gateway

- OE Authentication Gateway is a Secure Token Server (STS).
- An STS provides Authentication Service, that returns an identity token upon successful validation of provided credentials.
- OpenEdge Authentication Gateway ensures trusted identity management by hardening the security of your OpenEdge application environment.
No access without being authenticated

Enforced by our STS run on the OpenEdge Authentication Gateway Server

ABL Client*

// Requests are redirected to STS
// Code requires valid CP

Access unlocked with a valid client principal

Directory Information Service
(e.g. LDAP, Active Directory)

Option to have DB locked
Unified Authentication for any access

- ABL Clients
- Application Server
- OpenEdge SQL Server
- Directory Information Service (e.g. LDAP, Active Directory)
- OpenEdge Database
OpenEdge Security Infrastructure

Web Mobile

HTTP

Web Server

HTTPS

Apache IIS

HTTP

Digital Certificate

Application Server

HTTPS

Progress Application Server for OpenEdge

or

Classic WebSpeed

Web Services

Digital Certificate

.NET

Java

OE GUI

OpenEdge Security Infrastructure

Web Speed

Open AS

WSAS

Database Server

ODBC

JDBC

SQL

OE CHUI

Transparent Data Encryption

Authentication Gateway

STS

DB Connector

Authenticate

Encrypt

Decrypt
Contribution of OEAG to your solution

- Establish a single point of authorization, easy to manage, track, document and audit.
- Preclude inconsistent permissions
- Easily show, that any other access is impossible.
- Easily manage user identity in modern service-oriented and multi-tier applications by an identity credential (client principal) that is tightly integrated into the OpenEdge architecture.

OpenEdge Authentication Gateway

Centralizes authentication and authorization service for database access, providing trusted identity management.
Managing Data
Seven Key Considerations

- Do you collect, process and store personal data?
- How is personal data secured in your application, including when it is in transit and at rest?
- What technology do you have in place to ensure proper authentication and authorization access to personal data, both internally and externally?
- How do you track manipulation of personal data?
- Can you ensure that personal data is handled consistently across systems?
- Do you support companies that collect, store and process personal data?
- How is handling personal data automated and governed by rules?
## Managing Personal Data

<table>
<thead>
<tr>
<th>OpenEdge Change Data Capture</th>
<th>OpenEdge Multi Tenant Tables</th>
<th>OpenEdge Replication</th>
<th>OpenEdge Management</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify, track and save personal data changes within the RDBMS and support accurate synchronization across the business</td>
<td>Ensure the separation of your customer data within the cloud, reducing development and deployment costs when delivering SaaS applications</td>
<td>Near real-time continuous duplication for fast data recovery, minimizing the impact of unexpected outages and supporting High Availability as part of a business continuity strategy</td>
<td>Proactive monitoring to identify anomalies in performance that may be the result of breach or unplanned outage</td>
</tr>
</tbody>
</table>
How do I ..?

- restrict access to personal data if servicing multiple organisations?
- keep personal data separate while running a shared installation in a computing center?
- make sure that I cannot access data by any ABL/SQL query outside the boundaries of my domain?
OpenEdge RDBMS Multitenancy

Ensure the separation of customer data accessible via the cloud, while reducing development and deployment costs when delivering SaaS applications.
Safe against tempering

- Multi-tenancy built into the database
- Data physically partitioned by tenant identity
- Tenants share same schema definition
- Minimal application changes
  - Just set a per-database tenant name
- Data can be stored physically on specific Storage Area (extents)
Access governed by Policies

- A tenant is a collection of users
- A user is a "person"
- A security domain is a named set of rules ("policies") for how a group of users identity and tenant association is verified
Contribution of Multi-Tenancy to your solution

▪ Provides a reliable and attestable infrastructure to keep personal data separate by design.

▪ Provides access by policies, which are easy to document and certify.

▪ Accelerates Saas deployment with minimal code change, still secure.
  • Authentication will link to the correct tenant

▪ Baseline: Personal Data is kept private by Tenant.

OpenEdge Multi Tenant Tables

Ensure the separation of your customer data within the cloud, reducing development and deployment costs when delivering SaaS applications.
How do I ..?

- track, who changes personal data?
- control, which personal data gets shared and forwarded to other applications?
- Make sure, that data maintenance, requested by a user are applied to all copies? (e.g. purge a record, purge all copies)
OpenEdge Change Data Capture

Identify, track and save data changes within the RDBMS and support accurate data source synchronization across the business.

Data Extraction

- OpenEdge Change Data Capture
- Data Warehouse
- Operational Data Store
- Analytics
- Financial Systems
Entry point Database Administration

CDC enabled

- Change Data Capture Tables List
- Create Change Data Capture policy

Database Features
- Table Partitioning
- Read-only Partitions
- New VST Tables
- Multi-tenancy
- Large Keys
- Change Data Capture

Security Summary
- Blank user id access: Allowed
- Security administrator: Not defined
- Users: 0
- Domains: 5
- Disabled domains: 0

Storage Management
- Edit authentication systems
- Edit data security
- Review user data security

Data Administration
- Edit sequences
- Export sequences
- Load CDC policies (.cd file)
- Load table contents (.d file)
- Dump table contents (.d file)
- Dump CDC policies (.cd file)
- Dump group contents (.d file)
Change Capture controlled by Policies

- Select Tables and Fields
- Define the level of detail (0 to 3)
- Provides current status as well as history
CDC_customer table after an update

FOR EACH cdc_customer WHERE DATE(_Time-Stamp) = TODAY:

    DISP Name City Country _Operation _Time-Stamp WITH WIDTH 200.

END.

Fields before changes (operation = 3)

<table>
<thead>
<tr>
<th>Name</th>
<th>City</th>
<th>Country</th>
<th>_Operation</th>
<th>_Time-Stamp</th>
</tr>
</thead>
<tbody>
<tr>
<td>Lift Tours My Test</td>
<td>Burlington</td>
<td>?</td>
<td>3</td>
<td>15/11/2017 22:04:02, 630+01:00</td>
</tr>
<tr>
<td>Lift Tours</td>
<td>Burlington</td>
<td>?</td>
<td>4</td>
<td>15/11/2017 22:04:02, 630+01:00</td>
</tr>
<tr>
<td>Lift Tours</td>
<td>Burlington</td>
<td>UK</td>
<td>3</td>
<td>15/11/2017 22:05:00, 349+01:00</td>
</tr>
<tr>
<td>Lift Tours My change</td>
<td>Burlington</td>
<td>USA</td>
<td>4</td>
<td>15/11/2017 22:05:00, 349+01:00</td>
</tr>
</tbody>
</table>

Fields after changes (operation = 4)
Contribution of CDC to your solution

- Automatically and safely synchronize (update and delete) personal data across systems
- Define the scope of personal data, that may get shared by policies, that are easy to document.
- Data Economy: By a history of policies you can prove that only the necessary amount of data got shared.
Privacy by Design, Privacy by Default
Seven Key Considerations

- Do you collect, process and store personal data?
- How is personal data secured in your application, including when it is in transit and at rest?
- What technology do you have in place to ensure proper authentication and authorization access to personal data, both internally and externally?
- How do you track manipulation of personal data?
- Can you ensure that personal data is handled consistently across systems?
- Do you support companies that collect, store and process personal data?
- How is handling personal data automated and governed by rules?
How do I ..?

▪ apply legal obligations of GDPR to my application logic in an attestable, easy to read and understandable form?
▪ make sure, that I purge personal data as required by law and interpretation?
▪ obfuscate or blind (anonymize) data as stipulated?
▪ work with personal data using defined processes, that safeguard compliance?
▪ Respond to user or auditor requests in a reliable, transparent way?
Privacy by Design and Default

OpenEdge Business Process Management (BPM)

Improve processes to make informed decisions about how personal data is managed throughout the organization.

Corticon Rules Management for OpenEdge

Manage complex rules, including business rules designed to determine when it is necessary to delete personal data from your database when there is no longer a legitimate business reason to collect, process and/or store such data.
OpenEdge BPM in a Nutshell
Corticon BRMS for OpenEdge in a Nutshell
Contribution of BPM and Rules to your solution

- Rules that define how to process personal data are defined independent from your application code. -> easier to change and to document.

- Compulsory maintenance of personal data can be automated, in order to safeguard against violating GDPR related rules and obligations.

- Helps to track and document maintenance of personal data -> prove compliance.
OpenEdge Building Blocks of your Strategy

- Data Encryption
- Data Accuracy
- Cloud Scale and Manage
- Disaster Recovery
- Effective Resource Management
- Application Server
- Identity Management
- Business Rules Management

New Enhancements: OpenEdge 11.7

Available in the Advanced Enterprise Edition
Get ready for GDPR: Mission Possible!
Security by Design / an example

• Long term Application partner
• Developing HR Software, 600 Customers
• Including some administration agencies providing HR and other services to large client firms.
• Current security features home grown not certifiable, not compliant with legal requirements
• Risk of Service not passing the next business auditing
Security by Design / an example

• Auditing tracks changes to personal data.
• Multi-Tenancy will provide built-in client data separation, that cannot be tampered by ABL Coding
• Transparent Data Encryption with multiple keys will protect data against intrusion attempts
• Authentication Gateway integrates the application’s user permission control layer into the agencies’ central User Management
• Progress AppServer for OpenEdge will provide a standardized security layer for self-service access
Next Steps

▪ Talk to your corporate legal team today, if you haven’t already
▪ Conduct a gap analysis of your business and technology, including your OpenEdge application
▪ Determine where your OpenEdge application may require upgrades to better address requirements
▪ Continue to reassess – it is not a point in time occurrence
▪ Join the Progress Community for discussing technical solutions
▪ Contact Progress for help with employing the features highlighted today
Learn More

Progress OE GDPR Page
https://www.progress.com/openedge/gdpr

Forrester Report: “Five Milestones to GDPR Success”
Available on the OE GDRP Page

EUGDPR.org

Regional IT Associations
Questions?