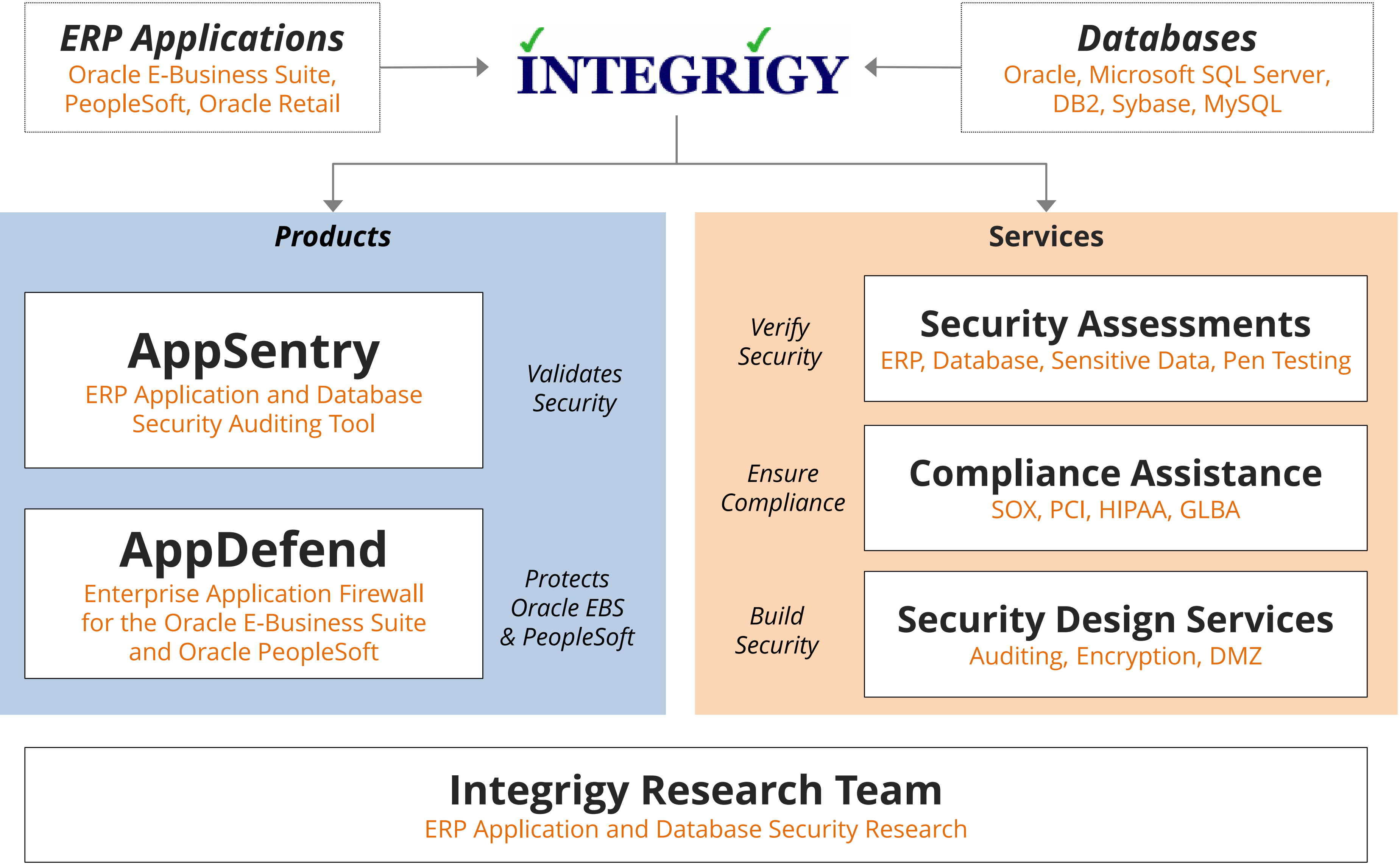
GDPR Compliance and the Oracle E-Business Suite Revisited

January 17, 2019

Stephen Kost
Chief Technology Officer
Integrigy Corporation

Phil Reimann
Director of Business Development
Integrigy Corporation

About Integrigy



ERP Applications

Oracle E-Business Suite, PeopleSoft, Oracle Retail

INTEGRIGY

Databases

Oracle, Microsoft SQL Server, DB2, Sybase, MySQL

Products

AppSentry

ERP Application and Database Security Auditing Tool

Validates Security

AppDefend

Enterprise Application Firewall for the Oracle E-Business Suite and Oracle PeopleSoft

Protects Oracle EBS & PeopleSoft

Services

Verify Security

Security Assessments

ERP, Database, Sensitive Data, Pen Testing

Ensure Compliance

Compliance Assistance

SOX, PCI, HIPAA, GLBA

Build Security

Security Design Services

Auditing, Encryption, DMZ

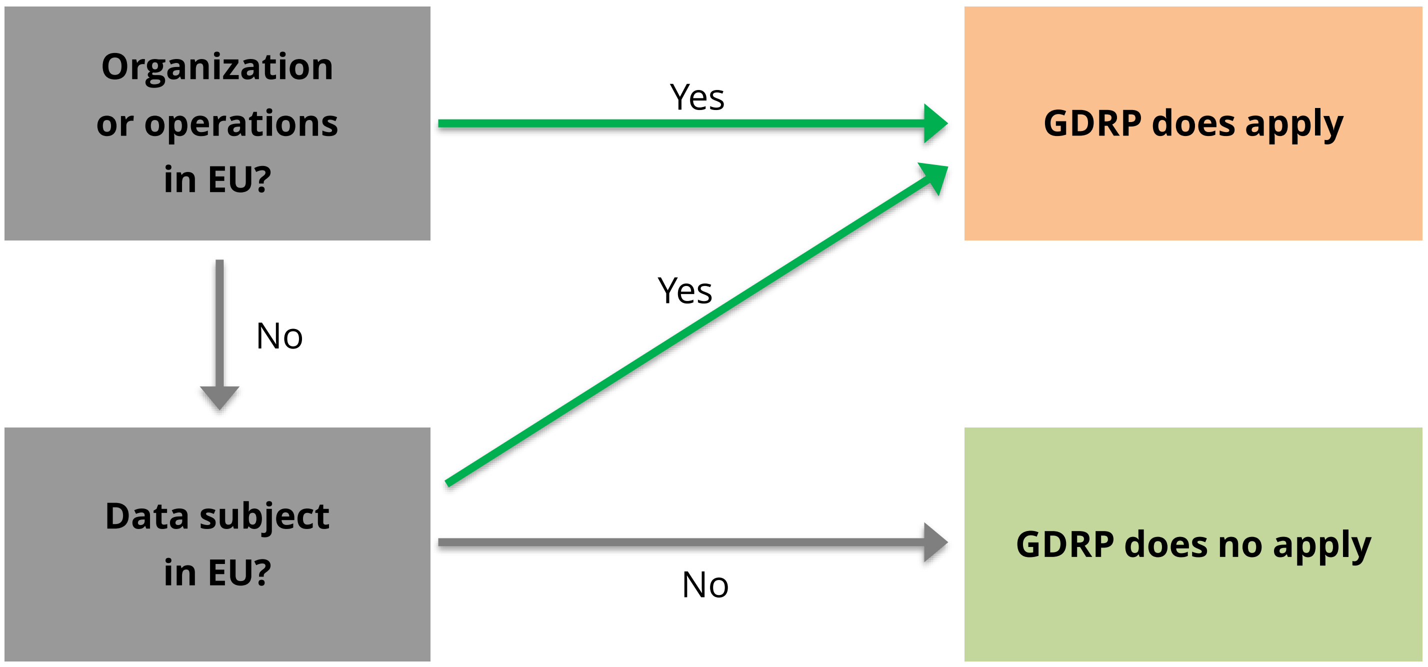
Integrigy Research Team

ERP Application and Database Security Research

GDPR =
General Data Protection Regulation

Who	European Union (EU)
What	Protect **EU citizen and resident** data
Where	**Everywhere** EU data resides
When	**25 May 2018** enforcement date

GDPR Organization Scope



GDPR Data Subjects

- Employees
- Contractors
- Customers
- Clients
- Suppliers
- Vendors

Data Scope

Any information that can be used to **identify an individual directly or indirectly.** This could be data of clients, employees, suppliers, stakeholders, etc.

Personal	Identifiers	Financial	Health
Name Age Address E-mail address Resume Religious affiliation Fingerprints Biometric data	Bank account number Credit card number Social Security number National identifier Financial account number Driver license number State ID number Tax identifier	Account balances Salary information Pay stubs Tax withholding Tax payments	Protected health info Medical conditions Physical characteristics Medical test results Mental health evaluations Provision of health care Payments for health care

Article 83 – Non-Compliance Fines

In the case of non-compliance
the organization risks fines of up to
4% of the annual global turnover
or **€20M**, whichever is greater

Article 33/34 – Breach Notification

Data breaches must be reported to The Data Protection Authority (DPA) **within 72 hours** (where feasible) and affected individuals must be informed of the breach “without undue delay.”

GDPR Main Tenets

- Rights of EU Data Subjects
- Security of Personal Data
- Lawfulness and Consent
- Accountability
- Data Protection by Default and by Design – Article 25

GDPR Rights of EU Data Subjects - Articles 12 - 23

- Right to access their personal data
- Right to update their data
- Right to restrict the use of their data
- Right to erasure (to be forgotten)
- Right to port their data to another Processor

ARTICLE

24 Evidence and Compliance

> ...demonstrate that the processing of personal data is performed in compliance with this Regulation.

- **39 of the 99 GDPR articles require Evidence to demonstrate compliance.**
- **Must maintain audit trails for evidence and forensics.**
- **Prove that security controls are functioning properly over a period of time – not just at the time of a static audit.**
- **GDPR mandates accountability within the organization and has well-defined roles like “Data Protection Officer” and “Controller”.**

ARTICLE

32 Comprehensive Security

In assessing the appropriate level of security, account shall be taken in particular of the risks that are presented by processing, in particular from accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to personal data transmitted, stored or otherwise processed.

- **A layered-security approach is critical for GDPR compliance.**
- **For Oracle EBS, must include all layers of the technology stack including application, database, application server, operating system, and network.**
- **Use the “Secure Configuration Guide for Oracle E-Business Suite” (MOS Note ID 403537.1) as a starting point.**
- **Develop a comprehensive security standard for EBS and all technology stack layers.**
- **Must continually assess compliance with security standard.**

ARTICLE

32 Pseudonymization and Encryption

> … shall implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, … (a) The pseudonymization and encryption of personal data; (b) the ability to ensure the ongoing confidentiality, integrity, availability …

- **A key goal of GDPR is that anonymization and pseudonymization of data can reduce the risk of accidental or intentional data disclosure by making the information un-identifiable to an individual or entity.**

Production	Test/Development
• Scan for sensitive data using data scanner – must know where all data elements are. • Enable EBS encryption for credit card numbers and bank account numbers. • Encrypt tablespaces using Oracle TDE ($$$).	• Purge personal data whenever possible – very difficult to do. • Scramble all personal data when cloning from production – many tables and columns.

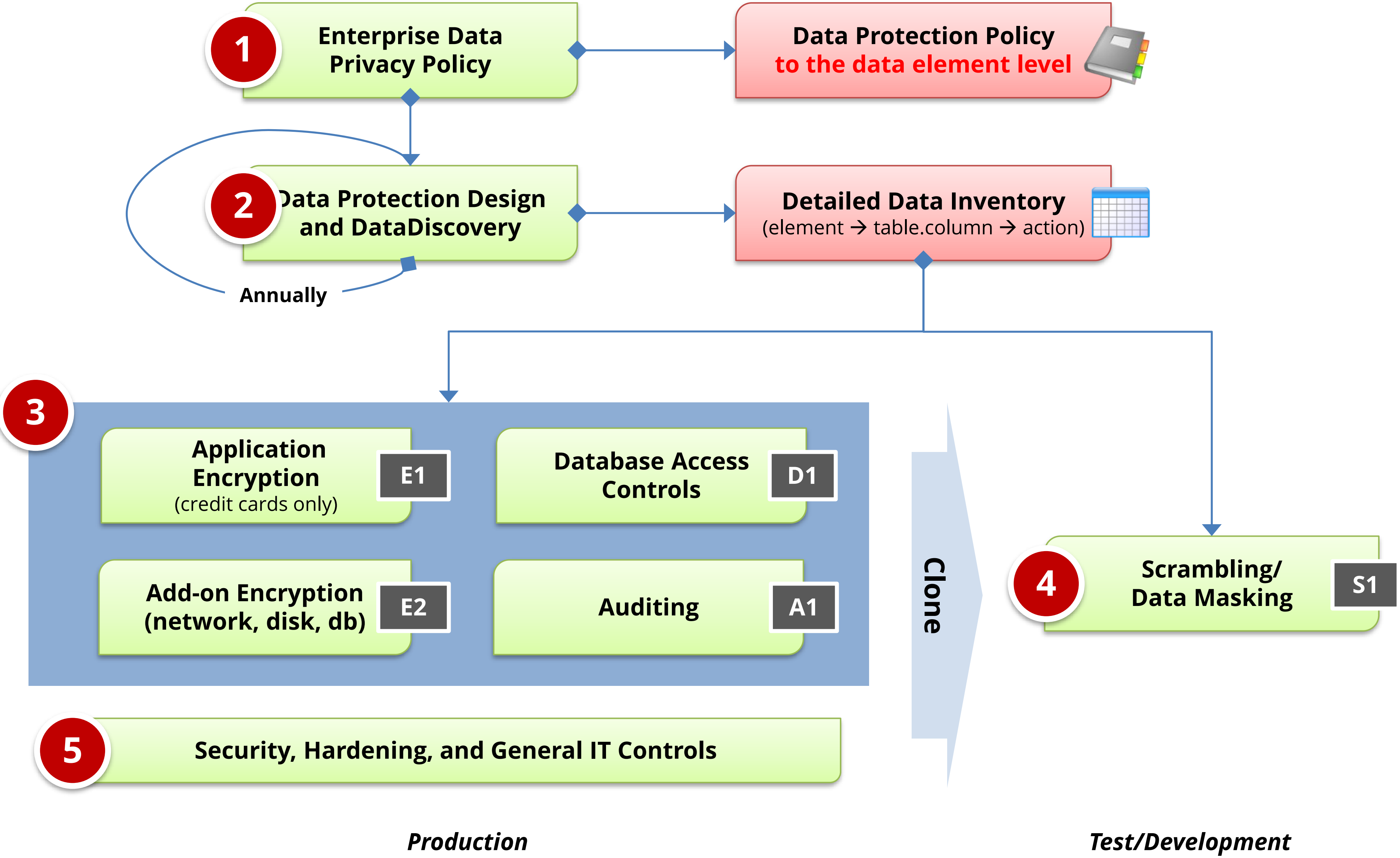
ARTICLE

25 Data Protection by Design and by Default

Controller shall implement appropriate technical and organizational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed.

- Data access must use preventative controls whenever possible.
- All GDPR data access must be defined by role and purpose of access and limited to those individuals.
- DBA access is a significant challenge – may require Database Vault.
- Must perform quarterly access reviews for both EBS and database to validate technical and organizational measures are functioning properly.

Integrigy Data Protection Process



1 Enterprise Data Privacy Policy

Data Protection Policy
to the data element level

2 Data Protection Design and DataDiscovery

Annually

Detailed Data Inventory
(element → table.column → action)

3

Application Encryption
(credit cards only)
E1

Database Access Controls
D1

Add-on Encryption (network, disk, db)
E2

Auditing
A1

Clone

4 Scrambling/ Data Masking
S1

5 Security, Hardening, and General IT Controls

Production

Test/Development

Where is GDPR Data in Oracle EBS?

Credit Card Data	iby_security_segments (encrypted) ap_bank_accounts_all oe_order_headers_all aso_payments oks_k_headers_* oks_k_lines_* iby_trxn_summaries_all iby_credit_card
Social Security Number (National Identifier) (Tax ID)	per_all_people_f hr_h2pi_employees ben_reporting ap_suppliers ap_suppliers_int po_vendors_obs
Bank Account Number	ap_checks_all ap_invoice_payments_all ap_selected_invoice_checks_all
Protected **Health Information (PHI)**	Order Management Accounts Receivables Human Resources

Where else might be GDPR Data?

Custom tables

- Customizations may be used to store or process sensitive data

“Maintenance tables”

- DBA copies tables to make backup prior to direct SQL update
- hr.per_all_people_f_011510

Interface tables

- Credit card numbers are often accepted in external applications and sent to Oracle EBS

Oracle EBS Flexfields

- It happens – very hard to find

Database

Interface files

- Flat files used for interfaces or batch processing

Log files

- Log files generated by the application (e.g., iPayment)

File System

ARTICLE

29 User Access Control

> … Processor and any person … who has access to personal data, shall not process those data except on instructions from the Controller…

- **User access control (UAC) is addressed at the application and database layers – distinct level of controls for each layer.**
- **Segregation of duties (e.g., SOX) does not address data access – must have a separate review of application responsibilities for access to GDPR data elements.**
- **Database access review is as critical as the application as database users – often generic and highly privileged (SELECT ANY TABLE) – usually have unlimited access to data.**
- **Must maintain audit trails of at least high-level access by named individual and any changes to these privileges at the application and database layer.**

Article

30 Audit Trail

Each Controller …. shall maintain a record of processing activities under its responsibility.

- **Oracle EBS audit trails and database auditing must be enabled, protected, and archived.**
- **Must monitor in near real-time for data breaches (notification within 72 hours).**
- **Audit trail must include access to GDPR data elements by named individuals, access to privileged accounts, changes to access rights or security controls, and changes to security configuration.**
- **A centralized logging and monitoring system must be used in order to properly “maintain a record” as well as monitor for breaches.**

Data Protection vs. Threats

Data Access Method and Threats	Options						
	1 EBS Encrypt	2 Trigger View	3 Oracle TDE	4a FGAC	4b Internal Audit	4c External Audit	3 + 4 TDE + Auditing
1. Application access by end-users (responsibility)	E	E		C	A	A	A
2. Application access by application administrators	E+	E-		C	A	A	A
3. Database access by DBA	E	E		C	A+	A	A
4. Database access by Applications DBA (SYSTEM, APPS)	E+	E+			A+	A+	A+
5. Database access by other database accounts	E	E		C	A	A	A
6. Operating system access to database data files	E	E	E				E
7. On-line or off-line access to database backups	E	E	E				E
8. Exploitation of Oracle Applications security vulnerabilities	E-	E-		C+	A+	A+	A+
9. Exploitation of Oracle Database security vulnerabilities	E+	E+		C+	A+	A+	A+
10. Exploitation of operating system security vulnerabilities	E	E	E				E

E = Encrypted, **C** = Access Controlled, **A** = Access Audited, **+** = Mostly **-** = Partially

ARTICLE

5 Data Minimization

Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed ('data minimization').

- **Oracle EBS is limited in data minimization capabilities – purge functionality is not available for all GDPR data elements.**
- **Must have defined standards per data element as to the purpose and relevance including retention time, right to be forgotten, and requirements for access.**

"[Oracle] does not recommend third-party tools for data subsetting in EBS environments. Third-party tools are pretty-much guaranteed to destroy referential integrity within an EBS database, and such usage will be treated like an invasive customization." -- EBS ATG Oracle Development

ARTICLE

17 Right to Erasure ('right to be forgotten')

> The controller shall have the obligation to erase personal data without undue delay when: … (b) the data subject withdraws consent.

- **For 12.1.3 and 12.2.3+ only, Oracle has introduced the Oracle EBS Person Data Removal Tool (PDRT). Patch released on April 18, 2018 – see MOS Doc ID 2388237.1.**
- **If the person has transactions, “the data removal is primarily focused on overwriting and obfuscating selected data in place.”**
- **If the person has no transactions, the person records are removed.**

HR Person	TCA Party	FND_USER
Employee Ex-Employee Contingent Worker Ex-Contingent Worker Applicant Other Person	Customer Customer Contact Supplier Supplier Contact	USER_ID

GDPR Data Scope Identification

Integrigy SQL queries to identify GDPR in-scope data –

https://integrigy.com/solutions/gdpr

- HR Employees
- Contingent Workers
- Applicants
- HR Other Persons
- Customers
- Customer Contacts
- Suppliers
- Supplier Contacts

Integrigy GDPR Scripts Sample Output

```
BE     Applicant             2
BE     Contact               2
BE     Employee              37
BE     Expatriate            1
DE     Employee              12
DE     Expatriate            1
DE     Foreign Employee      1
DK     Applicant             20
DK     Contact               2
DK     Employee              76
ES     Applicant             2
ES     Contact               2
ES     Employee              2
FI     Applicant             20
FI     Contact               2
FI     Employee              152
…
```

References

- General GDPR Information
- Gdpr-info.eu
- Eugdpr.org

- Oracle and GDPR
- Oracle GDRP Resource Center – https://www.oracle.com/applications/gdpr/index.html

- Oracle E-Business Suite and GDPR
- Product Feature Guide: GDPR and Oracle EBS MOS Note ID 2363912.1
- Oracle EBS Purging and Archiving of Data MOS Note ID 2073624.1
- Oracle EBS Person Data Removal Tool MOS Note ID 2388237.1

Contact Information

Stephen Kost

Chief Technology Officer

Integrigy Corporation

web: **www.integrigy.com**

e-mail: **info@integrigy.com**

blog: **integrigy.com/oracle-security-blog**

youtube: **youtube.com/integrigy**