The EU General Data Protection Regulation and how Oracle can help

Gusztáv Szuhai
Security Solutions / CE
Oracle
Currently...

Single EU Directive (Directive 95/46/EC) has not prevented fragmentation in the way Data Protection is implemented.

Outdated: Not prepared for the Cloud, Big Data & Social

Tough to be competitive in a market where compliance is not streamlined.
EU Digital Single Market Initiative

2 Parts

GDPR: General Data Protection Regulation

General Regulation of the EU (digital) market

DPD: Data Protection Directive

Directive for data handling during police or court processes and in cases authorities of the EU member states exchange PII
Benefits for **Citizens**

- Right to be forgotten
- Decide how your data is used
- Easier access to your own data
- Right to know you have been hacked
- Data Protection First
It’s not only about EU Data Protection

contains requirements for

Static
- Encryption
- Hardening
- Patching
- Configuration Lifecycle

Dynamic
- Authentication
- Authorisation
- Auditing
- Administration

confidentiality
availability
integrity
1. Records of processing

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility (A.30)

- A list documenting for each processing:
  - Purposes of processing (eg. personal appraisal)
  - Description of categories of data subjects (eg. employees)
  - Categories of personal data (eg. performance and potential)
  - Information related to transfers to a third country and international organization (eg. USA - Oracle Talent cloud service)
  - Time limits for erasure (eg. end of work relationship + 1 months)
  - Description of security measures (eg. level 3 measures in MyGroup procedure XY, + CASB)

- Records of processing should be perceived as the starting point for IT security in the framework of GDPR compliance

- Should be used as a working tool to achieve and control compliance

- Can be used to demonstrate compliance and accountability

- Can be modular extended with more information
2. Risk and Data protection impact assessment

The word “Risk” is used 75 times in this Regulation: the controller and processor must understand and reduce the risk for data subject

• Furthermore when the processing is likely to result in a high risk to the rights and freedoms of natural persons a formal Data Protection Impact Assessment (A.35) is required, prior of the processing, to:
  – Define the security measures to apply
  – Understand if it is necessary to consult the Data Protection Authority and seek approval

• Article 29 Data Protection Working Party (WP29) published the Guidelines on Data Protection Impact Assessment (DPIA)

• The DPIA is a tool for managing risks to the rights of the data subjects, and thus takes their perspective whereas risk management in some other fields (e.g. information security) is focused on the organization.

• These guidelines make a reference to international best practices such as ISO 31000:2009, Risk management — Principles and guidelines, and ISO/IEC 29134 (project), Information technology — Security techniques — Privacy impact assessment — Guidelines
3. Articles related to the rights of the data subject

Chapter 3 “Rights of the data subject” (Section 2 and 3) provide a list of obligations for the controller

- Right of access by the data subject (A.15)
- Right to rectification (A.16)
- Right to erasure (‘right to be forgotten’) (A.17)
- Right to restriction of processing (A.18)
- Notification obligation regarding rectification or erasure of personal data or restriction of processing (A.19)
- Right to data portability (A.20)

These articles require often human intervention and/or application modification, for example:

- Erasure shall be evaluated taking into account other subjects’ rights and laws including for example pending invoices still to be paid (human intervention)
- Data portability requires a function to export in a machine-readable format the data requested by the data subject (application modification)
4. Articles related to security measures

Several articles make reference to the obligation to adopt appropriate technical and organisational measures

- Principles relating to processing of personal data (A.5)
- Responsibility of the controller (A.24)
- Data protection by design and by default (A.25)
- Processor (A.28)
- Security of processing (A.32)
- Communication of a personal data breach to the data subject (A.34)

The most explanatory is article 32 (Security of processing) because it gives better information about this topic, including:

- Context and objectives
- An example of a security measure (encryption)
- Indications about the goals to achieve
- Elements that may be used to demonstrate compliance

Security measures can be often implemented in the architecture.
A typical path towards EU GDPR compliance

- **DPO nomination**
- **Maintain (create) the record of processing (art 30)**
- **Data protection impact assessment (art 35)**
- **Assess & Discover (data, systems and risks)**
- **Security of processing (art 32)**
- **Rights:**
  - Application and Systems modifications to guarantee rights of data subject (art 15-20)
  - Obligation: Data protection by design and by default (art 25)
- **Implement: Enforce & Enrich (security measures and processes)**
- **Notification of personal data breaches to the supervisory authority (art 33), and communication to the data subject (art 34)**
Several Oracle products or security cloud services can help to achieve compliance to GDPR.

We can help to:

1. Discover sensitive data with data governance solutions
2. Enforce data, software and identity security
3. Enrich application functions to guarantee rights of data subjects
4. Support a foundation that includes good IT practices, and high availability and resilience
A path towards GDPR – technology domains

Several Oracle products or security cloud services can help to achieve compliance to GDPR.

We can help to:
1. Discover sensitive data with data governance solutions
2. Enforce data, software and identity security
3. Enrich application functions to guarantee rights of data subjects
4. Support a foundation that includes good IT practices, and high availability and resilience
## A path towards GDPR – detailed product mapping

### Maintain (Create) a Record of Processing (A.30)

<table>
<thead>
<tr>
<th>Product / Suite</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 Enterprise Manager - Automatic Discovery</td>
</tr>
<tr>
<td>2 Enterprise Metadata Management</td>
</tr>
<tr>
<td>3 Enterprise Data Quality</td>
</tr>
<tr>
<td>4 Application Data Modeling - Sensitive Data Discovery</td>
</tr>
<tr>
<td>5 Identity Governance</td>
</tr>
<tr>
<td>6 Access Management</td>
</tr>
<tr>
<td>7 Centralized Directory</td>
</tr>
<tr>
<td>8 Identity Cloud Service</td>
</tr>
<tr>
<td>9 Database Vault</td>
</tr>
<tr>
<td>10 Advanced Security and Key Vault</td>
</tr>
<tr>
<td>11 Database Masking and Subsetting</td>
</tr>
<tr>
<td>12 Audit Vault &amp; DB Firewall</td>
</tr>
<tr>
<td>13 Security Monitoring and Analytics</td>
</tr>
<tr>
<td>14 Cloud Access Security Broker</td>
</tr>
<tr>
<td>15 Enterprise Manager - Configuration and Compliance pack</td>
</tr>
<tr>
<td>16 Configuration and Compliance Cloud Service</td>
</tr>
<tr>
<td>17 Data Guard and Real Application Cluster</td>
</tr>
<tr>
<td>18 Exadata and Supercluster</td>
</tr>
<tr>
<td>19 Zero Data Loss Recovery Appliance &amp; ZFS</td>
</tr>
<tr>
<td>20 SPARC / Solaris</td>
</tr>
<tr>
<td>21 Customer Data Management Cloud Service</td>
</tr>
<tr>
<td>22 Policy Automation</td>
</tr>
<tr>
<td>23 Analytics Cloud</td>
</tr>
<tr>
<td>24 BI Enterprise Edition</td>
</tr>
<tr>
<td>25 Data Integration</td>
</tr>
</tbody>
</table>

### Adapt Incident Response Process (A.33; A.34) and Company Risk Practices Including DPIA (A.35)

1. **Create Systems and Software Inventory**

2. **Discover Sensitive Data**

3. **Application and Data Scope is Available and Incrementally Defined**


5. **Secure Configuration**

6. **Monitor, Block and Audit**

7. **Protect the Data**

8. **Access Control**

### Evaluate Required Application Modifications to Guarantee Rights of Data Subject (A.15-20)

9. **Data Guard and Real Application Cluster**

10. **Exadata and Supercluster**

11. **Zero Data Loss Recovery Appliance & ZFS**

12. **SPARC / Solaris**

13. **Customer Data Management Cloud Service**

14. **Policy Automation**

15. **Analytics Cloud**

16. **BI Enterprise Edition**

17. **Data Integration**

### Enforce Good IT and Good Security Across the Stack (A.32, A.25)

18. **Enforce Good IT and Good Security Across the Stack**

GDPR – Security of Processing

- **Protect the Data**: Protect data wherever it resides and avoid using real data where it’s not necessary.
- **Access Controls**: Modernize IDM to guarantee authentication of business users and IT personnel.
- **Monitor, Block and Audit**: Collect, consolidate, secure, and analyze audit logs.
- **Secure Configuration**: Secure Configurations, remediate vulnerabilities, and control production baselines.
Prevent Damage to Databases from Attacks

Data Encryption

Key Vault

Data Redaction
dob:xx/xx/xxxx
ssn:xxx-x-4321

DB Controls
Access denied
Sensitive Data, IP PCI, PII, PHI

Data Subsetting
Region, Year Size-based

Dev/Test Partners, BI

Data Masking
dob: 12/01/1987
11/05/1999

Privileged User

Applications

Users

CX App

Sensitive Data, IP PCI, PII, PHI

Prevent Damage to Databases from Attacks

Key Vault

Data Encryption

*7#$%!@%!afb
#<>*$#@34

Data Redaction
dob:xx/xx/xxxx
ssn:xxx-x-4321

DB Controls
Access denied
Sensitive Data, IP PCI, PII, PHI

Data Subsetting
Region, Year Size-based

Dev/Test Partners, BI

Data Masking
dob: 12/01/1987
11/05/1999

Privileged User

Applications

Users

CX App

Sensitive Data, IP PCI, PII, PHI

Prevent Damage to Databases from Attacks

Key Vault

Data Encryption

*7#$%!@%!afb
#<>*$#@34

Data Redaction
dob:xx/xx/xxxx
ssn:xxx-x-4321

DB Controls
Access denied
Sensitive Data, IP PCI, PII, PHI

Data Subsetting
Region, Year Size-based

Dev/Test Partners, BI

Data Masking
dob: 12/01/1987
11/05/1999

Privileged User

Applications

Users

CX App

Sensitive Data, IP PCI, PII, PHI
Oracle Security Portfolio

• **Database Security**
  – Oracle Advanced Security
    • Data at rest encryption
    • Data Redaction
  – Oracle Key Vault
    • Key Management (Creation, renewal/rollover...)
  – Oracle Database Vault
    • Protection against privileged users e.g. DBA
  – Oracle Audit Vault Database Firewall
    • Central warehouse of log records from multi-vendor database and non-databases
    • Protection against SQL Injection attacks (multi-vendor databases)
  – Oracle Label Security
    • Extra protection for very important rows
  – Data Masking
    • Masking of sensitive data outside of production

• **Identity and Access Management**
  – Oracle Identity Governance
    • User lifecycle management (joiners, movers, leavers)
  – Oracle Access Management
    • Single sign-on, 2FA
  – Oracle Directory Services
    • LDAP offering (including virtualised Directory)

• **Security Cloud Services**
  – DB Cloud can make use of DB security features/options
    • Some options must be deployed on-premise
  – Oracle Identity Cloud Service
  – Oracle Cloud Access Security Broker (CASB) Cloud Service
  – Oracle Security Monitoring and Analytics Cloud Service
  – Oracle Configuration and Compliance Cloud Service
  – Oracle API Platform Cloud Service
Oracle Security Portfolio

• Database Security
  – Oracle Advanced Security
    • Data at rest encryption
    • Data Redaction
  – Oracle Key Vault
    • Key Management (Creation, renewal/rollover...)
  – Oracle Database Vault
    • Protection against privileged users e.g. DBA
  – Oracle Audit Vault Database Firewall
    • Central warehouse of log records from multi-vendor database and non-databases
    • Protection against SQL Injection attacks (multi-vendor databases)
  – Oracle Label Security
    • Extra protection for very important rows
  – Data Masking
    • Masking of sensitive data outside of production

• Identity and Access Management
  – Oracle Identity Governance
    • User lifecycle management (joiners, movers, leavers)
  – Oracle Access Management
    • Single sign-on, 2FA
  – Oracle Directory Services
    • LDAP offering (including virtualised Directory)

• Security Cloud Services
  – DB Cloud can make use of DB security features/options
    • Some options must be deployed on-premise
  – Oracle Identity Cloud Service
  – Oracle Cloud Access Security Broker (CASB) Cloud Service
  – Oracle Security Monitoring and Analytics Cloud Service
  – Oracle Configuration and Compliance Cloud Service
  – Oracle API Platform Cloud Service
Oracle Security Portfolio

- **Database Security**
  - **Oracle Advanced Security**
    - Data at rest encryption
    - Data Redaction
  - **Oracle Key Vault**
    - Key Management (Creation, renewal/rollover...)
  - **Oracle Database Vault**
    - Protection against privileged users e.g. DBA

- **Identity and Access Management**
  - Oracle Identity Governance
    - User lifecycle management (joiners, movers, leavers)
  - Oracle Access Management
    - Single sign-on, 2FA
  - Oracle Directory Services
    - LDAP offering (including virtualised Directory)

- **Security Cloud Services**
  - DB Cloud can make use of DB security features/options
    - Some options must be deployed on-premise
  - Oracle Identity Cloud Service
  - Oracle Cloud Access Security Broker (CASB) Cloud Service
  - Oracle Security Monitoring and Analytics Cloud Service
  - Oracle Configuration and Compliance Cloud Service
  - Oracle API Platform Cloud Service
Oracle Security Portfolio

- **Database Security**
  - Oracle Advanced Security
  - Data at rest encryption
  - Data Redaction
  - Oracle Key Vault
  - Key Management (Creation, renewal/rollover...)
- **Oracle Database Vault**
  - Protection against privileged users e.g. DBA
  - Oracle Audit Vault Database Firewall
    - Central warehouse of log records from multi-vendor database and non-databases
    - Protection against SQL Injection attacks (multi-vendor databases)
  - Oracle Label Security
    - Extra protection for very important rows
- **Data Masking**
  - Masking of sensitive data outside of production

- **Identity and Access Management**
  - Oracle Identity Governance
    - User lifecycle management (joiners, movers, leavers)
  - Oracle Access Management
    - Single sign-on, 2FA
  - Oracle Directory Services
    - LDAP offering (including virtualised Directory)

- **Security Cloud Services**
  - DB Cloud can make use of DB security features/options
    - Some options must be deployed on-premise
  - Oracle Identity Cloud Service
  - Oracle Cloud Access Security Broker (CASB) Cloud Service
  - Oracle Security Monitoring and Analytics Cloud Service
  - Oracle Configuration and Compliance Cloud Service
  - Oracle API Platform Cloud Service
Detect, Audit and Monitor

- Database Firewall
  - Users
  - Applications
  - Alerts
  - Reports
  - Policies
  - Network Events
  - Audit Data
  - Audit Data, Event Logs

- Databases
  - Oracle
  - IBM
  - MySQL
  - Sybase
  - Microsoft
  - Solaris
  - Linux
  - Windows Server
  - New
Oracle Security Portfolio

**Database Security**
- Data at rest encryption
- Data Redaction
- Oracle Key Vault
  - Key Management (Creation, renewal/rollover...)
- Oracle Database Vault
  - Protection against privileged users e.g. DBA
- Oracle Audit Vault Database Firewall
  - Central warehouse of log records from multi-vendor database and non-databases
  - Protection against SQL Injection attacks (multi-vendor databases)
- Oracle Label Security
  - Extra protection for very important rows
- Data Masking
  - Masking of sensitive data outside of production

**Identity and Access Management**
- Oracle Identity Governance
  - User lifecycle management (joiners, movers, leavers)
- Oracle Access Management
  - Single sign-on, 2FA
- Oracle Directory Services
  - LDAP offering (including virtualised Directory)

**Security Cloud Services**
- DB Cloud can make use of DB security features/options
  - Some options must be deployed on-premise
- Oracle Identity Cloud Service
- Oracle Cloud Access Security Broker (CASB) Cloud Service
- Oracle Security Monitoring and Analytics Cloud Service
- Oracle Configuration and Compliance Cloud Service
- Oracle API Platform Cloud Service
Oracle Security Portfolio

- **Database Security**
  - Oracle Advanced Security
    - Data at rest encryption
    - Data Redaction
  - Oracle Key Vault
    - Key Management (Creation, renewal/rollover...)
  - Oracle Database Vault
    - Protection against privileged users e.g. DBA
  - Oracle Audit Vault Database Firewall
    - Central warehouse of log records from multi-vendor database and non-databases
    - Protection against SQL Injection attacks (multi-vendor databases)
  - Oracle Label Security
    - Extra protection for very important rows
  - Data Masking
    - Masking of sensitive data outside of production

- **Identity and Access Management**
  - Oracle Identity Governance
    - User lifecycle management (joiners, movers, leavers)
  - Oracle Access Management
    - Single sign-on, 2FA
  - Oracle Directory Services
    - LDAP offering (including virtualised Directory)

- **Security Cloud Services**
  - DB Cloud can make use of DB security features/options
    - Some options must be deployed on-premise
  - Oracle Identity Cloud Service
  - Oracle Cloud Access Security Broker (CASB) Cloud Service
  - Oracle Security Monitoring and Analytics Cloud Service
  - Oracle Configuration and Compliance Cloud Service
  - Oracle API Platform Cloud Service
Oracle Security Portfolio

**Database Security**
- **Oracle Advanced Security**
  - Data at rest encryption
  - Data Redaction

**Oracle Key Vault**
- Key Management (Creation, renewal/rollover...)

**Oracle Database Vault**
- Protection against privileged users e.g. DBA

**Oracle Audit Vault Database Firewall**
- Central warehouse of log records from multi-vendor database and non-databases
- Protection against SQL Injection attacks (multi-vendor databases)

**Oracle Label Security**
- Extra protection for very important rows

**Data Masking**
- Masking of sensitive data outside of production

**Identity and Access Management**
- Oracle Identity Governance
  - User lifecycle management (joiners, movers, leavers)
- Oracle Access Management
  - Single sign-on, 2FA
- Oracle Directory Services
  - LDAP offering (including virtualised Directory)

**Security Cloud Services**
- DB Cloud can make use of DB security features/options
  - Some options must be deployed on-premise
- Oracle Identity Cloud Service
- Oracle Security Monitoring and Analytics Cloud Service
- Oracle Configuration and Compliance Cloud Service
- Oracle API Platform Cloud Service

---

Oracle Security Portfolio

1. Database Security
   - Oracle Advanced Security
     - Data at rest encryption
     - Data Redaction

2. Oracle Key Vault
   - Key Management (Creation, renewal/rollover...)

3. Oracle Database Vault
   - Protection against privileged users e.g. DBA

4. Oracle Audit Vault Database Firewall
   - Central warehouse of log records from multi-vendor database and non-databases
   - Protection against SQL Injection attacks (multi-vendor databases)

5. Oracle Label Security
   - Extra protection for very important rows

6. Data Masking
   - Masking of sensitive data outside of production

---

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. | 24
Maximum Security Architecture

Users
- Database Firewall
- Network Encryption
- Strong Authentication

Applications
- Database Firewall
- Network Encryption
- Audit Vault
- Users
- Applications

Events
- Audit Data & Event Logs
- Fine-Grained Access Controls
  - Database Vault
  - Virtual Private Database
  - Label Security
  - Real Application Security

Alerts
- Reports
- Policies

Enterprise Manager
- Single Sign-on using Oracle Identity Management
- Network Encryption
- Key Vault
- Data Encryption

Database Security Controls
- Assessment
- Preventive
- Detective

Copyright © 2014, Oracle and/or its affiliates. All rights reserved. | Oracle Public
Introducing Oracle Database Security Assessment Tool
Oracle Database Security Assessment Tool (DBSAT)

Assess Your Security Profile

• Understand how (in)secure your database is
  – Report on overall security status
  – Find the users, entitlements, and risks
  – Discover sensitive data

• Actionable Assessment Reports
  – Summary and detailed information
  – Prioritized recommendations
  – Mapping to EU GDPR and CIS Benchmark

• Stand-alone light weight tool: Quick, Easy

• FREE to current Oracle customers
What does DBSAT Check?

1. **Security Configuration**
   - Data Encryption
   - Auditing Policies
   - Fine-grained Access Control
   - Database and Listener Configuration
   - OS File permissions
   - Security Patches

2. **Users and Entitlements**
   - User Accounts, Privileges and Roles

3. **Sensitive Data**
   - Which type, where, how many

For Oracle Databases 10g and later
Report in Multiple Formats

**HTML**

```
USER.DEFPWD
Status: High Risk
Summary: Found 2 unlocked user accounts with default password.
Details: Users with default password: HR, SCOTT
Remarks: Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.
References: CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2
```

**JSON**

```
...
"severity": 5,
"title": "Users with Default Passwords",
"remarks": "Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well."
"details": "Users with default password: HR, SCOTT",
"refs": [
{"CIS": "Recommendation 1.2"}
],
"type": "finding",
"id": "USER.DEFPWD",
"summary": "Found 2 unlocked user accounts with default password."
},...
```

**Spreadsheet**

<table>
<thead>
<tr>
<th>Users with Default Passwords</th>
<th>CIS</th>
<th>USER.DEFPWD</th>
<th>High Risk</th>
<th>Found 2 unlocked user accounts with default password.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Minimum Client Authentication</td>
<td>USER.AUTHVER</td>
<td>$</td>
<td>Low Risk</td>
<td>Minimum client version is not configured correctly.</td>
</tr>
</tbody>
</table>

**Text**

```
Users with Default Passwords: HR, SCOTT

Default account passwords for predefined Oracle accounts are well known. Open accounts with default passwords provide a trivial means of entry for attackers, but well-known passwords should be changed for locked accounts as well.

References: CIS Oracle Database 12c Benchmark v2.0.0: Recommendation 1.2
```
Try it today

- [DBSAT OTN page](#)
- [#DBSAT on Social Networks](#)

- Database Security and GDPR Whitepaper [https://go.oracle.com/LP=54366](https://go.oracle.com/LP=54366)
- Know more about GDPR [www.oracle.com/goto/gdpr](http://oracle.com/goto/gdpr)
Oracle Consulting EU GDPR Assessment and Roadmap

**Overview**

**Objective:** Help customer in assessing their organization’s readiness against security requirements for EU GDPR. Help customer define a roadmap to secure their most critical systems and to implement key security components.

**Duration:** up to 5 days

**What We Do:** Oracle security architects will lead you through a wide-ranging analysis of your IT security policies, operations and procedures, and security controls. We’ll work with your key security and EU GDPR stakeholders including data owners, and IT systems managers to assess your environment, future requirements and identify gaps in order to provide recommendations and best practices.

**Learn More**

**Typical Deliverables:**
- Assessment questionnaires with key findings, gap analysis of critical systems against the EU GDPR security requirement baseline
- EU GDPR IT enablement maturity levels for data protection in the existing architecture
- Recommend security capabilities with key benefits for each
- Reference architecture blueprint
- Implementation roadmap and cost indication
- Executive summary presentation

**Benefit:**
- Help you accelerating compliance with EU GDPR security requirements
- Demonstrate the value and benefits of Oracle Security Cloud services and On-Premise products in your IT context
- Identify quick wins while providing a roadmap and cost estimate to implement overall necessary security capabilities
The Three Pillars of Security Controls

**People Security**
- Authentication
- Governance
- Audit

**Software Security**
- Application and Service Configuration
- IT Compliance
- API Security
- Application and Service Performance
- Patching
- Audit

**Data Security**
- Preventative Controls
- Encryption
- Segregation of Duty
- Data Masking
- Administrative Controls
- Detective Controls
- Audit

**Threat Intelligence, User/Log Analytics, Incident Response**
Oracle Solutions That May Assist with EU-GPDR Compliance

Database Security

<table>
<thead>
<tr>
<th>GDPR Term</th>
<th>Oracle Database Security Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption</td>
<td>Encryption &amp; Redaction</td>
</tr>
<tr>
<td>Pseudonymous Data</td>
<td>Key Management</td>
</tr>
<tr>
<td>Limited Access to Data</td>
<td>Data Masking</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>Label-based Data Security</td>
</tr>
<tr>
<td>Breach Notification</td>
<td>Auditing, SQL Injection</td>
</tr>
<tr>
<td></td>
<td>Segregation of Duties</td>
</tr>
<tr>
<td></td>
<td>Sensitive Data Discovery</td>
</tr>
</tbody>
</table>
## Oracle Solutions That May Assist with EU-GPDR Compliance

### Software Security

<table>
<thead>
<tr>
<th>GDPR Term</th>
<th>Security Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor &amp; Assess</td>
<td>Cloud Access Security Broker Cloud Service</td>
</tr>
<tr>
<td>User Identification</td>
<td>Configuration and Compliance Cloud Service</td>
</tr>
<tr>
<td>Access to Data</td>
<td>Security Monitoring and Analytics Cloud Service</td>
</tr>
<tr>
<td>Unified Access Enforcement</td>
<td>API Platform Cloud Service</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td></td>
</tr>
</tbody>
</table>

GDPR Term:
- Risk Assessment
- Unified Access Enforcement
- Access to Data
- User Identification
- Monitor & Assess

Security Cloud Services:
- Cloud Access Security Broker Cloud Service
- Configuration and Compliance Cloud Service
- Security Monitoring and Analytics Cloud Service
- API Platform Cloud Service
Oracle Solutions That May Assist with EU-GPDR Compliance

People Security

<table>
<thead>
<tr>
<th>GDPR Term</th>
<th>Oracle IAM Solutions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Monitor &amp; Assess</td>
<td>Identity CS</td>
</tr>
<tr>
<td>User Identification</td>
<td>IAM Monitoring</td>
</tr>
<tr>
<td>Access to Data</td>
<td>Access Management</td>
</tr>
<tr>
<td>Unified Access Enforcement</td>
<td>Identity Governance</td>
</tr>
<tr>
<td></td>
<td>Directory Services</td>
</tr>
</tbody>
</table>

Oracle Solutions That May Assist with EU-GPDR Compliance
Oracle Solutions that May Assist with GDPR compliance

<table>
<thead>
<tr>
<th>Data protection by design and by default - Art. 25</th>
<th>How Oracle Technology may assist</th>
<th>Oracle Products/Security Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement appropriate technical and organizational measures, such as pseudonymization, which are designed to</td>
<td><strong>Data Security</strong></td>
<td>Oracle Database Security</td>
</tr>
<tr>
<td>implement data-protection principles, such as data minimization in an effective manner and to integrate the</td>
<td>To protect <em>Personal Data</em> in new or existing applications by deploying appropriate database security products.</td>
<td>Oracle DBCS High/extreme performance</td>
</tr>
<tr>
<td>necessary safeguards into the processing in order to meet the requirements of this Regulation and protect the</td>
<td>To mask (pseudonymization) copies of production <em>Personal Data</em> used in test and development</td>
<td>Oracle Data Masking</td>
</tr>
<tr>
<td>rights of data subjects</td>
<td>environments to reduce the risk of exposure of <em>Personal Data</em>.</td>
<td></td>
</tr>
<tr>
<td></td>
<td>To redact <em>Personal Data</em> e.g. Date-of-birth can be redacted e.g. <strong>-</strong>-1985 to minimise access to <em>Personal Data</em> via applications.</td>
<td>Oracle Advanced Security</td>
</tr>
</tbody>
</table>
## Oracle Solutions that May Assist with GDPR compliance

<table>
<thead>
<tr>
<th>Data protection by design and by default - Art. 25 (continued)</th>
<th>How Oracle Technology may assist</th>
<th>Oracle Products/Security Cloud Services</th>
</tr>
</thead>
</table>
| Ensure that, by default, personal data are not made accessible without the individual’s intervention to an indefinite number of people | **People Security**  
To provision only the **right** people (employees, contractor, customers, partners) with access to the **right** *Personal Data* at the **right** time. | Oracle Identity Governance Suite  
Oracle Access Management Suite  
Oracle Identity Cloud Service |
| **Software Security**  
Ensure visibility, configuration and threat protection for Cloud Services.  
Protect APIs from misuse.  
Ensure Applications and Cloud Services are configured properly.  
Ensure applications and Cloud Services that process *Personal Data* should be monitored for intrusions/misuse by attackers (including insiders). | | Oracle CASB Cloud Service  
Oracle API Platform Cloud Service  
Oracle Configuration and Compliance Cloud Service  
Oracle Security Monitoring and Analytics Cloud Service |
## Oracle Solutions that May Assist with GDPR compliance

<table>
<thead>
<tr>
<th>Security of Processing - Art. 32</th>
<th>How Oracle Technology may assist</th>
<th>Oracle Products/Security Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:</td>
<td><strong>Data Security</strong>&lt;br&gt;To mask <em>Personal Data</em> outside of production databases.&lt;br&gt;To encrypt <em>Personal Data</em> stored in, and travelling to and from Oracle databases.&lt;br&gt;To manage keys used to encrypt databases containing <em>Personal Data.</em>&lt;br&gt;To protect against privileged users&lt;br&gt;To protect against SQL injection attacks on databases containing <em>Personal Data.</em>&lt;br&gt;To replicate <em>Personal Data</em>&lt;br&gt;To enable hot standby of <em>Personal Data</em>&lt;br&gt;To enable resilience of processing&lt;br&gt;To protect databases on Oracle Cloud</td>
<td>Oracle Data Masking&lt;br&gt;Oracle Advanced Security&lt;br&gt;Oracle Key Vault&lt;br&gt;Oracle Database Vault&lt;br&gt;Oracle Audit Vault Database Firewall&lt;br&gt;Oracle Data Guard&lt;br&gt;Oracle Real Application Clusters&lt;br&gt;Oracle Zero Data Loss Recovery Appliance&lt;br&gt;Oracle DBCS High/extreme performance</td>
</tr>
</tbody>
</table>
## Oracle Solutions that May Assist with GDPR compliance

<table>
<thead>
<tr>
<th>Security of Processing - Art. 32</th>
<th>How Oracle Technology may assist</th>
<th>Oracle Products/Security Cloud Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Implement appropriate technical and organizational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:</td>
<td><strong>People Security</strong>&lt;br&gt;To manage lifecycles of users accessing <em>Personal Data</em>.</td>
<td>Oracle Identity Governance</td>
</tr>
<tr>
<td>(a) the pseudonymization and encryption of personal data;</td>
<td>To centralise authentication of users accessing <em>Personal Data</em></td>
<td>Oracle Access Management&lt;br&gt;Oracle Directory Services&lt;br&gt;Oracle Identity Cloud Service</td>
</tr>
<tr>
<td>(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;</td>
<td><strong>Software Security</strong>&lt;br&gt;To ensure visibility, configuration and threat protection for Cloud Services. &lt;br&gt;To protect APIs providing access to <em>Personal Data</em></td>
<td>Oracle CASB Cloud Service</td>
</tr>
<tr>
<td>(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident</td>
<td>To monitor application and service configuration</td>
<td>Oracle API Platform Cloud Service</td>
</tr>
<tr>
<td></td>
<td>To monitor and respond to anomalous behaviour relating to applications processing <em>Personal Data</em></td>
<td>Oracle Configuration and Compliance Cloud Service&lt;br&gt;Oracle Security Monitoring and Analytics Cloud Service</td>
</tr>
</tbody>
</table>
## Oracle Solutions that May Assist with GDPR compliance

<table>
<thead>
<tr>
<th>Security Breach/Notification to Data Subjects - Art. 34</th>
<th>How Oracle Technology may assist</th>
<th>Oracle Products/Security Cloud Services</th>
</tr>
</thead>
</table>
| The controller is exempt from notifying the data subjects about a high risk breach if the controller can demonstrate to the SA that it has implemented appropriate information security measures that render the data unintelligible to any person not authorized to access it (e.g. via encryption) or taken measures to mitigate the high risk for data subjects | **Data Security**  
Protect databases | Oracle Advanced Security  
Oracle Key Vault  
Oracle Database Vault  
Oracle Audit Vault Database Firewall |
| | **People Security**  
Protect applications  
Manage user access | Oracle Access Management  
Oracle Identity Governance  
Oracle Directory Services |
| | **Software Security**  
Ensure visibility, configuration and threat protection for Cloud Services.  
Protect APIs from misuse.  
Monitor/remEDIATE configurations.  
DevOps security management. Security log analytics. | Oracle CASB Cloud Service  
Oracle API Platform Cloud Service  
Configuration and Compliance Cloud Service  
Security Monitoring and Analytics Cloud Service |
## Oracle Solutions that May Assist with GDPR compliance

<table>
<thead>
<tr>
<th>General conditions for imposing administrative fines - Art. 83</th>
<th>How Oracle Technology may assist</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following: ... the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;</td>
<td>See Oracle technology related to Articles 25 and 32 above</td>
</tr>
</tbody>
</table>