GDPR for the Oracle DBA

Prepare for May 2018
Pete Finnigan – Background, Who Am I?

- Oracle Security specialist and researcher
- CEO and founder of PeteFinnigan.com Limited in February 2003
- Writer of the longest running Oracle security blog
- Oracle ACE for security
- Member of the OakTable
- Speaker at various conferences  
  - UKOUG, PSOUG, BlackHat, more..
- Published many times, see  
  - [http://www.petefinnigan.com](http://www.petefinnigan.com) for links
- Influenced industry standards  
  - And governments
Agenda

• Disclaimer
• What is GDPR – Overview?
• How does GDPR impact the Oracle database and its practitioners?
• What tools, techniques and solutions can help with GDPR compliance in the Oracle database?

We can only cover the GDPR at a high level in around 33 slides and 45 minutes.
Disclaimer

• I am not a lawyer
• GDPR is a law
• This presentation is not legal advice and is not intended to be legal advice – do no treat it as such
• This presentation is my interpretation of some of GDPR and how the Oracle DBA will be involved
• Do not rely on the contents of this presentation as a complete overview of everything in the GDPR – it is not intended to be and is intended to highlight certain aspects only in a non-legal way.
GDPR

- General Data Protection Regulation (GDPR) (Regulation EU 2016/679)
- Replaces the data protection derivative 95/46/EC in 1995
- Adopted by EU 27 April 2016
- Enforceable from 25th May 2018 (10 Days time!!)
- Does not require national governments to pass any enabling legislation so is binding straight away in May 2018
- Each member state will establish a Supervising Authority (SA)
- Authority in the UK it will be the ICO (Information Commissioners Office)

See https://gdpr-info.eu for details
The Scary Parts

- 20M Euro or 4% of companies GDP fines for breach
- It is incredibly complex – over 100 Pages, 11 Chapters, 99 Articles, notes (Recitals)…
- Do the law makers understand how much time and money this will costs companies to investigate and implement?
- Brexit will not stop GDPR for UK companies
- Will Affect non EU countries who process EU persons data
- Most companies will need to do something
- The SME get out in the data protection act seems to have been removed
- **Have you started? Where to start?**
Lots of Views on GDPR

- A search for GDPR shows 16.3 Million results (8M in December)
- I have been emailed over 30 articles, webinars, papers and more on GDPR in the last couple of months alone (December)
  - Now every day at least 4 offers of GDPR services, training and more
- I have read many papers even in esoteric magazines
  - Airline, communications (telephones) and more
Oracle suggests in this paper [http://www.oracle.com/technetwork/database/security/wp-security-dbsec-gdpr-3073228.pdf](http://www.oracle.com/technetwork/database/security/wp-security-dbsec-gdpr-3073228.pdf) that the following products can help with GDPR:

**We can achieve a lot of similar results with core options as well**

- Encryption (TDE) (ASO)
- Data Redaction (ASO)
- OEM Application modeller
- Database Vault privilege analysis
- OEM life cycle management pack
- Key vault
- Label security
- Audit Vault and DB firewall
- IAM products
- Data masking
- Database Vault SOD
- Real Application Security (RAS)
- DBSAT
- VPD
- ASO for SSL
- Database auditing
- FGA
- VPD and TSDP
Oracle Database / GDPR Mapping

• Not everything in GDPR article maps nicely to issues or functions in the Oracle database

• Some “Articles” in GDPR may have an affect on the Oracle database

• Some issues / GDPR Challenges across the database may be part of multiple articles

• Some products may help solve some of the GDPR issues

• It is not a straight cut mapping between one or more products and GDPR compliance

• **Let's look at some of the key GDPR Articles that affect data in an Oracle database**
Article 4: Definitions

- Personal Data means any information that relates to an identified or identifiable natural person (The Data subject).
- An identifiable person is one that can be identified directly or indirectly by a name, id, online id, IP Address or many other factors such as social, physical, mental, economic, religion and more.
- Profiling is any automated processing of personal data.
- Pseudonymisation is processing personal data in a way that the data cannot be attributed to a specific data subject without additional data – this data should be held separately.
Article 35: Data Protection and Impact Assessment

• Carry out an impact assessment of the personal data processed
• A single assessment can be used for similar processing areas
• Also if necessary carry out and make the impact assessment on data that does not require an impact assessment
• The assessment shall also include current security measures
• Make the impact assessment list public
• The ICO (in the UK) can request to see this
Article 25: Data Protection by Design and Default

- All processing of personal data shall include technical and organisational techniques such as
  - Pseudonymisation of data (encrypt, mask…)
  - Data minimisation
  - Only data necessary for purpose are held and processed
  - Limit the period of storage and accessibility
  - Technical measures should be used to ensure that personal data is not made accessible (Data Security)
- Privacy by design; privacy by default

Protect and secure data in the database
Article 32: Security of Processing

• “Implement appropriate technical and organisational measures to ensure a level of security appropriate to risk”
• Pseudonymisation
• Encryption
• Ensure Confidentiality, Integrity, Availability and Resilience of processing systems
• Ability to restore access to personal data in event of an incident
• Process for regular testing and assessing of the security of processing (scanning for vulnerabilities)

Ensure that the database is secured and scanned for vulnerabilities and non-compliance on a regular basis.
Article 30: Records of Processing Activities

- Maintain a record of processing activities including:
  - Name and contact details of controller and DPO
  - Purpose of processing
  - Description of categories of data subject and category of personal data
  - Categories of recipients including 3rd parties
  - Transfer to a third country or international organisation
  - Where possible the envisaged time limit for erasure of the different categories of data
  - A general description of the technical and organisational security measures
- Must be achieved in most part by constant auditing of data access
Articles 33 and 34: Data Breach Notification

- A process must be in place to notify a breach within 72 hours of becoming aware of it to the regulator
- The breach must be investigated and details provided of the nature of the breach, consequences and mitigations to address it (fixes)
- If a high risk to individuals rights and freedoms the company will need to inform individuals without “undue delay”
- If the data is encrypted or otherwise obfuscated then individuals may not need to be informed
Articles 16 – 21: Data Subjects Rights

• Right to rectification of inaccurate data
• Right to erasure; right to be forgotten; where date is no longer necessary for the subject it was collected.
  • The company must be able to identify other data controllers it has sent data to
• Right to restriction of processing to verify accuracy of data, where processing is illegal but data subject does not want erasure, the controller does not need the data but the data subject requires it to be kept for legal claims
• Right to data portability in a format to take to another data controller
• Right to object to processing based on public interest or direct marketing

Add the ability (tools) to list personal data, delete it, extract it, target and fix it
Articles 5, 6, 15: Retention, Lawfulness, Access

- (Article 5): Data can only be retained for as long as is necessary for the purpose it was obtained.
  - The company needs to determine this length of time for all data before it is deleted or anonymised
- (Article 5): Employees should be trained in GDPR
- (Article 5): Policies should be created for data access, retention, data protection, breach escalation and checklist and more
- (Article 6): Legal grounds must be established for processing of non sensitive personal data held
- (Article 15): Does the company enable employees and customers to request their data processed
Who Needs to be Involved?

- If your Oracle database holds personal data you are involved
- A DBA, security person or anyone involved with Oracle day to day you will need to know something of GDPR
- One tenet of GDPR is appreciation, training and readiness
- How does GDPR affect or impact the Oracle database?
Tools, Techniques and Solutions

- Discover and document personal data
- Develop a security lock down process for the database in general
- Develop and assess data access controls to lock down access to personal data and user least privilege
- Scan the security of the database for compliance against the security policy
- Implement a detailed general audit trail policy
- Implement specific detailed personal data access audit policy
- Implement an incident response and forensics process
- Where necessary obfuscate, anonymise and encrypt data
- Deal with data subjects requests (automate)
Looking for Personal Data

• Identify the data to be searched for
• Look for tables of the right name (language variants)
• Look for columns of the right name (language variants)
• Sample all columns of type text and sample data
• Some data may be encrypted already
• Need to find 100% of data so look for duplicates
• Review the access rights on each data located
• Review any existing sweeping rights
• Review any existing audit trails
Sample – Search for Named Metadata

```sql
[SQL]> get ppl
  1 select owner, table_name
  2 from dba_tables
  3 where (table_name like '%PEOPLE%'
  4   or table_name like '%PERSON%'
  5   or table_name like '%NAME%'
  6   or table_name like '%INDIV%')
  7 and owner not in ('SYS', 'SYSMAN', 'MDSYS', 'SYSTEM')
  8* and owner not like 'APEX%'
[SQL> /

OWNER          TABLE_NAME
---------------  -------------------
ORABLOG         BOF_PERSON
```
Sample – Search for Sampled Data

```sql
-- find_data.sql
-- Copyright PeteFinnigan.com Limited 2017
-- Look for all tables with CHAR and VARCHAR2 columns and check for first names
--

declare
cursor c_col is
  select owner,table_name,column_name,data_type
  from dba_tab_columns
where owner='ORABLOG'
and data_type in ('CHAR','VARCHAR2')
and table_name not like 'BIN$%';
lv_cnt numbervariable:=0;
lv_stmt varchar2(32767):='';
begin
  for lv_col in c_col loop
    -- prepare the select
    lv_stmt:='select count(*) from ''||lv_col.owner||''.''||lv_col.table_name
    ||'' where ''||lv_col.column_name||'' in (''Pete',''Eric',''Emil'');
    -- dbms_output.put_line(''|lv_cluster'||''||lv_stmt||'''');  
    execute immediate lv_stmt into lv_cnt;
    if(lv_cnt>2) then
      dbms_output.put_line(lv_col.owner||''.''||lv_col.table_name
      ||'' may contain first names''||lv_col.column_name||'' may contain first names'';
    end if;
  end loop;
/
```

Search every schema for all different types of data; first name, last name, Post code, DOB, NI number.....
Sample – Search for All Data

This script can check each table for all access paths above it and also for copies of the same data and also list out access rights to all components.

Also need to check for sweeping access:
- SELECT ANY TABLE
- READ ANY TABLE
- INSERT ANY TABLE
- UPDATE ANY TABLE
- DELETE ANY TABLE
- CREATE ANY TRIGGER
- More…
get_tab2.sql shows rights granted on a table including those inherited via roles, via roles….
Develop a Plan to Secure The Database

- Develop a plan to include
  - Security patching (10%)
    - Patches should be applied consistently
  - Hardening (30%)
    - Important component of securing Oracle
    - Remove access to dictionary objects, parameters and add profiles etc
  - Design (60%)
    - Design work is complex
    - Data access controls
    - User rights
    - Context based security
    - Network controls and more

- Perform a detailed audit
- Develop a policy
- Secure the database
- Test compliance
Database Security Scanning

• Scan your database for security compliance
• Use free tools (DBSAT) or commercial tools (PFCLScan)
• Or free tools – write your own scripts

Oracle Database Security Risk Assessment

Assessment Date & Time

Date of Data Collection | Date of Report | Reporter Version
---|---|---
Tue Nov 08 2016 21:55:00 | Tue Nov 08 2016 21:22:49 | 1.0.3 (October 2016) - 7409

Database Identity

<table>
<thead>
<tr>
<th>Name</th>
<th>Platform</th>
<th>Database Role</th>
<th>Log Mode</th>
<th>Created</th>
</tr>
</thead>
<tbody>
<tr>
<td>BFORA</td>
<td>Linux x86 64-bit</td>
<td>PRIMARY</td>
<td>NOARCHIVELOG</td>
<td>Mon Apr 04 2016 07:36:00</td>
</tr>
</tbody>
</table>

Summary

<table>
<thead>
<tr>
<th>Section</th>
<th>Pass</th>
<th>Evaluate</th>
<th>Opportunity</th>
<th>Some Risk</th>
<th>Significant Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Basic Information</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>User Accounts</td>
<td>4</td>
<td>0</td>
<td>0</td>
<td>2</td>
<td>3</td>
</tr>
<tr>
<td>Privileges and Roles</td>
<td>6</td>
<td>12</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Authorization Control</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Data Encryption</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Fine-Grained Access Control</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Auditing</td>
<td>1</td>
<td>4</td>
<td>1</td>
<td>0</td>
<td>5</td>
</tr>
<tr>
<td>Database Configuration</td>
<td>4</td>
<td>0</td>
<td>2</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Network Configuration</td>
<td>1</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>3</td>
</tr>
<tr>
<td>Operating System</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>Total</td>
<td>17</td>
<td>22</td>
<td>6</td>
<td>7</td>
<td>14</td>
</tr>
</tbody>
</table>

Summary of Vulnerabilities

The table below shows the number of issues located in the database according to the severity of Critical, High, Medium, Low and informational. The number of issues located is also categorized per failed test and also the total number of issues located per check as a total. An indication is also given of the percentage security of the database in relation to the number of tests performed.

<table>
<thead>
<tr>
<th>Failed Checks</th>
<th>Issued Located</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>68</td>
</tr>
<tr>
<td>High</td>
<td>60</td>
</tr>
<tr>
<td>Medium</td>
<td>10</td>
</tr>
<tr>
<td>Low</td>
<td>0</td>
</tr>
<tr>
<td>Information</td>
<td>0</td>
</tr>
</tbody>
</table>

60.00%
begin
-- create the policy
atk.pfclatk.createpolicy('PROFILEPRIVILEGE');

-- audit profiles
atk.pfclatk.createandaddrule('PROFILEPRIVILEGE','Create Profile','CORE-S','create profile');
atk.pfclatk.createandaddrule('PROFILEPRIVILEGE','Drop Profile','CORE-S','drop profile');
atk.pfclatk.createandaddrule('PROFILEPRIVILEGE','Alter Profile','CORE-S','alter profile');
atk.pfclatk.createandaddrule('PROFILEPRIVILEGE','Profile','CORE-S','profile');

-- Add filter job to detect non-legitimate profile changes - i.e. use
-- of PROFILE system privileges; not use of statement PROFILE and not use
-- of a DBA IP address and not use of a DBA account; so if a DBA
-- uses a non DBA account from his own IP it should be detected

atk.pfclatk.addfilter('NON-AUTH-PROFILE-CHANGE','PROFILEPRIVILEGE','[Alert] Non-legitimate profile privilege change','select '''||a.action_name||'''

-- enable the policy
atk.pfclatk.enablepolicy('PROFILEPRIVILEGE');
end;
Right to be Forgotten – Delete data

![SQL query and output]

The 3C highlighted is the delete marker but the data is still there.
Anonymisation, Masking and Encryption

- Commercial solutions
  - TDE
  - Oracle Data Masking
  - Net 2000 – Data Masker – **Now Redgate Software**
  - Delphix
  - Oracle Redaction, VPD and TSDP
- Can we do for free?
  - Use encryption DBMS_CRYPTO
    - Key management is hard
    - No interfaces, GUI etc
    - No free masking solution but can generate masked data from scripts
Incident Response and Forensics

• Ensure that an incident plan exists
• Ensure that a team exists in advance who know and are trained to deal with an incident / attack
• Pre-gather tools and techniques to forensically analyse an attack
• Assume an attack will happen
• Enable a rich audit to capture abuse at the database engine level
• Establish a breach has occurred
Incident Response and Forensics - 2

- Locate the source of the attack
- Establish the time frame (start and end)
- Gather live artefacts (volatile) from server, database and other platforms
- Gather less volatile artefacts
- Perform forensic analysis
- Establish
  - How, as who, what was stolen, what was changed, the extent of access, what could they do with more skills?
Conclusions

- In general core database security (hardening and patching) will help towards GDPR
- Additional data access controls and least rights will help
- Audit controls are needed in general and on data
- Breach detection needed – use audit
- Incident response and forensics needed
- Some additional technologies from Oracle will certainly help BUT we can do a lot with free features as well
- Data impact assessment is a must
GDPR for the Oracle DBA

Prepare for May 2018