PFCL
PETEFINNIGAN.COM LIMITED

GDPR for the Oracle DBA

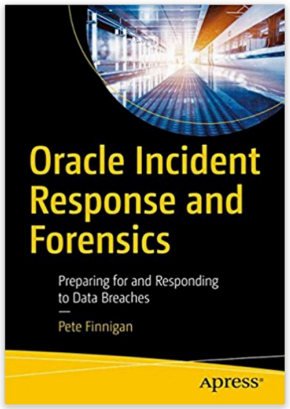
Prepare for May 2018

Legal Notice

GDPR for the Oracle DBA

Published by
PeteFinnigan.com Limited
Tower Court
3 Oakdale Road
York
England, YO30 4XL

PFCL
PETEFINNIGAN.COM LIMITED



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
- Author of the Oracle Security step-by-step guide and “Oracle Expert Practices”, “Oracle Incident Response and Forensics” books
- **Oracle ACE for security**
- **Member of the OakTable**
- Speaker at various conferences
  - UKOUG, PSOUG, BlackHat, more..
- Published many times, see
  - http://www.petefinnigan.com for links
- Influenced industry standards
  - And governments

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

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?

PFCL
PETEFINNIGAN.COM LIMITED

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.

See https://gdpr-info.eu for details

GDPR

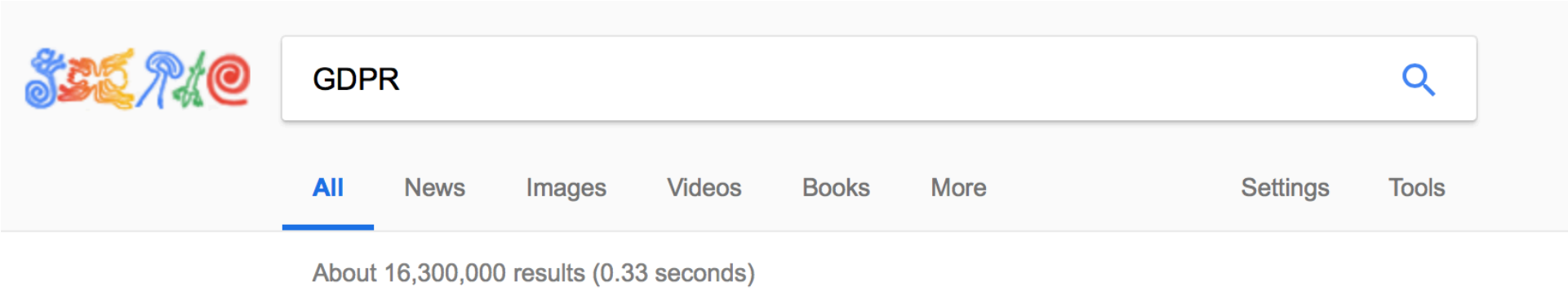
- General Data Protection Regulation (GDPR) (Regulation EU 2016/679)
- Replaces the data protection derivative 95/46/EC in 1995
- Adopted by EU 27 April 2016
- Enforceable from 25th May 2018 (**10 Days time!!**)
- Does not require national governments to pass any enabling legislation so is binding straight 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)

PFCL
PETEFINNIGAN.COM LIMITED

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

Oracles Mapping of GDPR

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

PFCL
PETEFINNIGAN.COM LIMITED

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
- **Lets 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

PFCL
PETEFINNIGAN.COM LIMITED

Locate and understand and document how personal data is stored and used

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
  - Pseudonnonymisation 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**

PFCL
PETEFINNIGAN.COM LIMITED

Ensure that the database is secured and scanned for vulnerabilities and non-compliance on a regular basis

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)

PFCL
PETEFINNIGAN.COM LIMITED

Implement Audit trails in the database

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

PFCL
PETEFINNIGAN.COM LIMITED

You must be able to detect a breach, analyse it and report it

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

PFCL
PETEFINNIGAN.COM LIMITED

Add the ability (tools) to list personal data, delete it, extract it, target and fix it

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

PFCL
PETEFINNIGAN.COM LIMITED

Delete data when not needed, know if its legal, train staff, list data

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

PFCL
PETEFINNIGAN.COM LIMITED

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?

PFCL
PETEFINNIGAN.COM LIMITED

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)

PFCL
PETEFINNIGAN.COM LIMITED

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> 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

SQL>
```

Develop queries to search for named tables or columns that hold metadata

Example for tables

Sample – Search for Sampled Data

```
-- 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 number:=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_stmt||']');
    execute immediate lv_stmt into lv_cnt;
    if(lv_cnt>2) then
      dbms_output.put_line(lv_col.owner||'.'||lv_col.table_name
          ||'.'||lv_col.column_name||' may contain first names');
    end if;
  end loop;
end;
/
```

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

```
SQL> @find_data
ORABLOG.BOF_PERSON.FIRST_NAME may contain first names
ORABLOG.BOF_PERSON_ENTITY_V.FIRST_NAME may contain first names

PL/SQL procedure successfully completed.
```

Sample – Search for All Data

```
SQL> @get_data


get_data: Release 1.1.0.0.0 - Production on Sun Dec 03 15:53:27 2017
Copyright (c) 2010, 2017 PeteFinnigan.com Limited. All rights reserved.

OBJECT TO CHECK                    [XXX_XXXX]: BOF_PERSON
SCHEMA/OWNER OF THE OBJECT TO CHECK   [USER]: ORABLOG
OUTPUT MODE [All,Equal]                  [E]:

Access to object, copies and children [ORABLOG.BOF_PERSON]
==================================================================


Tables to analyse [ORABLOG.BOF_PERSON]
==>
    ORABLOG.BOF_PERSON_ENTITY_V
    ORABLOG.BOF_PERSON_F
        ORABLOG.BOF_CUSTOMERS_ENTITY_V
        ORABLOG.BOF_EMPLOYEES_ENTITY_V
        ORABLOG.BOF_ORDERS_ENTITY_V
        ORABLOG.BOF_SHIPPING_ENTITY_V
---------------------------------------------


Main Table [ORABLOG.BOF_PERSON]
GRANTOR       GRANTEE        R S I U D A F D I R Q C E
------------- -------------- - - - - - - - - - - - - -
```

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…

Data Access Controls – Security of Data

```
SQL> @get_tab2


get_tab2: Release 1.2.0.0.0 - Production on Sun Dec 03 16:01:21 2017
Copyright (c) 2007, 2017, PeteFinnigan.com Limited. All rights reserved.

OBJECT TO CHECK                    [XXX_XXXX]: WP_USERS
SCHEMA/OWNER OF THE OBJECT TO CHECK   [USER]: ORABLOG
OUTPUT METHOD Screen/File                [S]:
FILE NAME FOR OUTPUT               [priv.lst]:
OUTPUT DIRECTORY [DIRECTORY  or file (/tmp)]:

Testing root object => [ORABLOG.WP_USERS]


GRANTOR       GRANTEE        R S I U D A F D I R Q C E
------------- -------------- - - - - - - - - - - - - -
ORABLOG       USER01           X
ORABLOG       USER03           X
ORABLOG       FACADM           X
ORABLOG       USER04           X
ORABLOG       USER02           X
ORABLOG       BACK01           X                        [,D][ORABLOG_READ]
ORABLOG       USER03           X                        [,D][ORABLOG_READ]
ORABLOG       USER04           X                        [,D][ORABLOG_READ]
ORABLOG       SYS              X                        [A,D][ORABLOG_READ]
ORABLOG       USER05           X                        [,D][ORABLOG_CREDIT][ORABLOG_READ]
ORABLOG       USER07           X                        [,D][ORABLOG_CREDIT][ORABLOG_READ]
ORABLOG       SYS              X                        [A,D][ORABLOG_CREDIT][ORABLOG_READ]
ORABLOG       USER06           X                        [,D][ORABLOG_CREDIT][ORABLOG_READ]
```

get_tab2.sql shows rights granted on a table including those inherited via roles, via roles….

PFCL
PETEFINNIGAN.COM LIMITED

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

PFCL
PETEFINNIGAN.COM LIMITED

Database Security Scanning

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

dbsat - Oracle... | osTicket :: Staf... | What does GD... | Recommendati... | DB Security As... | Document 145... | ORACLE-BASE... | odat/Ctxsys.py... | EM Express

Oracle Database Security Risk Assessment

Highly Confidential

Assessment Date & Time

Date of Data Collection	Date of Report	Reporter Version
Tue Nov 08 2016 21:05:00	Tue Nov 08 2016 21:22:49	1.0.2 (October 2016) - 7409

Database Identity

Name	Platform	Database Role	Log Mode	Created
BFORA	Linux x86 64-bit	PRIMARY	NOARCHIVELOG	Mon Apr 04 2016 07:36:00

Summary

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

[ForensicsProd] - PFCLScan : Database Security Audit Tool

PFCLReports [C:_aa\PD\PeteFinnigan.com Limited\PFCLScan\data\data\reporeports\505.1.20170919165449.single.htm]

PFCLScan Report Summary

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 categorised 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.

	Failed Checks	Errors Located
Critical	88	198
High	80	1160
Medium	30	36
Low	0	0
Information	0	0
	198	1394

60.00%

Implement Detailed Audit trails

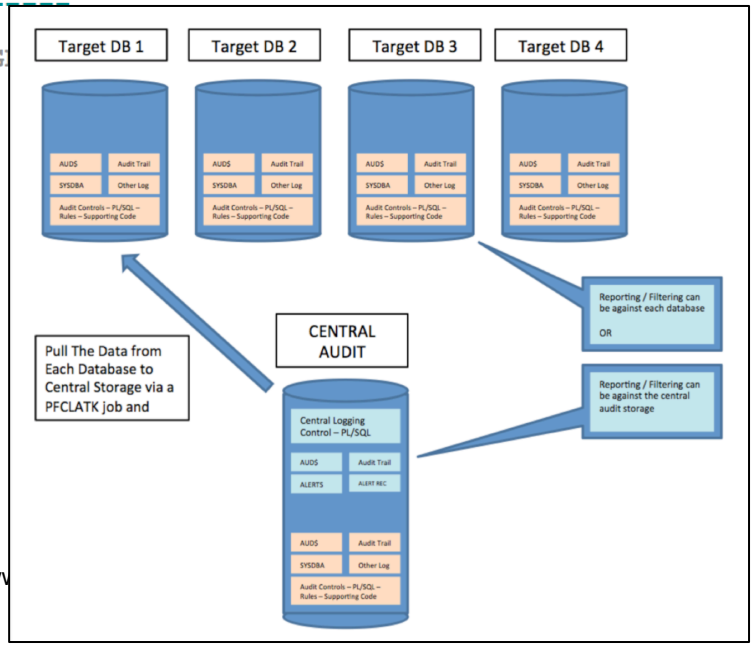
```
begin
  -- create the policy
  atk.pfclatk.createpolicy('PROFILEPRIVILEGE');

  -- 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-ligitimate 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 non-authorised user change {''||a.action_name||'

  -- enable the policy
  atk.pfclatk.enablepolicy('PROFILEPRIVILEGE');
end;
/
```



The 3C highlighted is the delete marker but the data is still there

Right to be Forgotten – Delete data

```
SQL> delete from scott.emp where empno=7934;

1 row deleted.

SQL> commit;

Commit complete.

SQL>
```

```
0012fd50h: 6A 61 76 61 78 2F 70 72 69 6
0012fd60h: 6C 61 76 6F 72 02 C1 02 FF 0
0012fd70h: 18 0C 2E 0D 07 78 71 08 18 0
0012fd80h: 18 0C 2E 0D 02 C1 02 FF FF 0
0012fd90h: 07 38 24 02 C1 02 2C 00 12 0
0012fda0h: 80 15 6A 61 76 61 78 2F 70 72 69 6E 74 2F 44 6F ; ..javax/print/Do
0012fdb0h: 63 46 6C 61 76 6F 72 02 C1 02 FF 02 C1 1E 07 78 ; cFlavor.Á.ÿ.Á..x
0012fdc0h: 71 08 18 0C 2E 3C 02 08 03 C2 50 23 06 4D 49 4C ; q....<...ÂP#.MIL
0012fdd0h: 4C 45 52 05 43 4C 45 52 4B 03 C2 4E 53 07 77 B6 ; LER.CLERK.ÂNS.w¶
0012fde0h: 01 17 01 01 01 02 C2 0E FF 02 C1 0B 2C 00 08 03 ; ......Â.ÿ.Á.,...
0012fdf0h: C2 50 03 04 46 4F 52 44 07 41 4E 41 4C 59 53 54 ; ÂP..FORD.ANALYST
0012fe00h: 03 C2 4C 43 07 77 B5 0C 03 01 01 01 02 C2 1F FF ; .ÂLC.wµ......Â.ÿ
0012fe10h: 02 C1 15 2C 00 08 02 C2 50 05 4A 41 4D 45 53 05 ; .Á.,...ÂP.JAMES.
0012fe20h: 43 4C 45 52 4B 03 C2 4D 63 07 77 B5 0C 03 01 01 ; CLERK.ÂMc.wµ....
0012fe30h: 01 03 C2 0A 33 FF 02 C1 1F 2C 00 08 03 C2 4F 4D ; ..Â.3ÿ.Á.,...ÂOM
0012fe40h: 05 41 44 41 4D 53 05 43 4C 45 52 4B 03 C2 4E 59 ; .ADAMS.CLERK.ÂNY
0012fe50h: 07 77 BB 05 17 01 01 01 02 C2 0C FF 02 C1 15 2C ; .w»......Â.ÿ.Á.,
0012fe60h: 00 08 03 C2 4F 2D 06 54 55 52 4E 45 52 08 53 41 ; ...ÂO-.TURNER.SA
0012fe70h: 4C 45 53 4D 41 4E 03 C2 4D 63 07 77 B5 09 08 01 ; LESMAN.ÂMc.wµ...
0012fe80h: 01 01 02 C2 10 01 80 02 C1 1F 2C 00 08 03 C2 4F ; ...Â....Á.,...ÂO
0012fe90h: 28 04 4B 49 4E 47 09 50 52 45 53 49 44 45 4E 54 ; (.KING.PRESIDENT
0012fea0h: FF 07 77 B5 0B 11 01 01 01 02 C2 33 FF 02 C1 0B ; ÿ.wµ......Â3ÿ.Á.
```

PFCL
PETEFINNIGAN.COM LIMITED

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

PFCL
PETEFINNIGAN.COM LIMITED

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

PFCL
PETEFINNIGAN.COM LIMITED

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?

PFCL
PETEFINNIGAN.COM LIMITED

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

PFCL
PETEFINNIGAN.COM LIMITED

GDPR for the Oracle DBA

Prepare for May 2018