
ORACLE®

GDPR a technológie
pomoc či prekážka súladu

Iveta Šťavinová
Oracle Slovensko
November 2017

ORACLE

Safe Harbor

Nasledujúci text je určený na načrtnutie nášho všeobecného smerovania produktov. Zameriava sa výhradne na informácie, a nesmie byť začlenený do akejkoľvek zmluvy. Nejedná sa o záväzok poskytnúť materiály, kód alebo funkcionalitu, a nemalo by sa naň spoliehať pri rozhodovaní o kúpe. Vývoj, uvoľňovanie a načasovanie všetkých funkcií alebo funkcionality popísaných pre produkty spoločnosti Oracle zostáva na základe výlučného rozhodnutia spoločnosti Oracle. Nie všetky identifikované technológie sú k dispozícii pre všetky Cloud služby.

Disclaimer

Informácie v tomto dokumente nesmú byť interpretované alebo použité ako právne poradenstvo týkajúce sa obsahu, interpretácie alebo aplikácie akéhokoľvek zákona, nariadenia alebo regulačného usmernenia. Zákazníci a potenciálni zákazníci musia hľadať vlastné právne poradenstvo, aby pochopili uplatniteľnosť akéhokoľvek zákona alebo nariadenia o spracovaní osobných údajov prostredníctvom použitia akéhokoľvek produktu alebo služieb dodávateľa

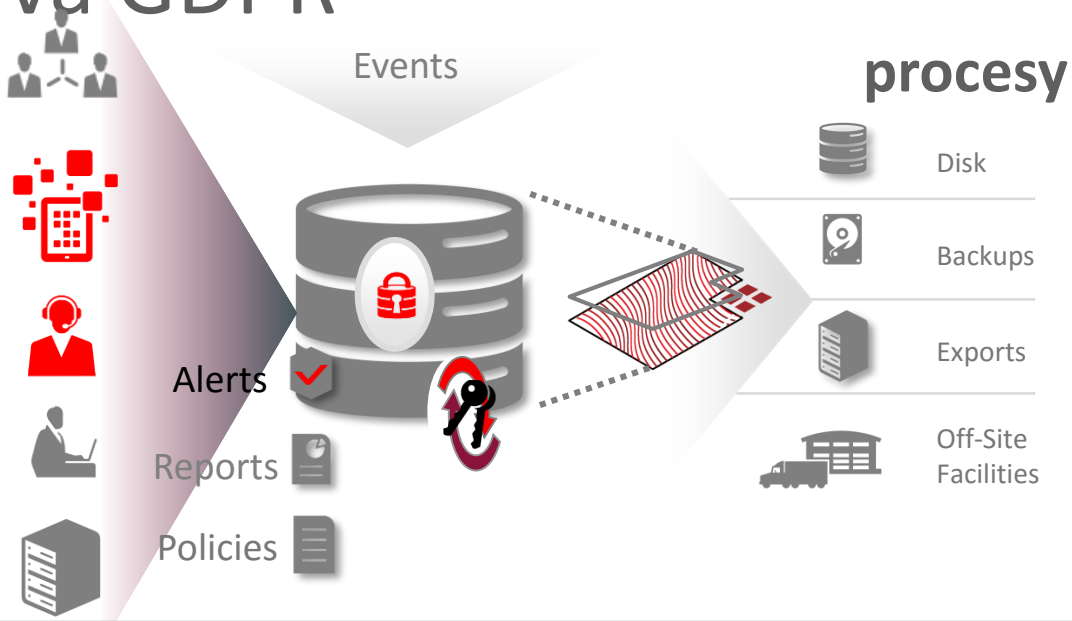
ORACLE

Štyri hlavné oblasti na ktoré vplýva GDPR

ľudia

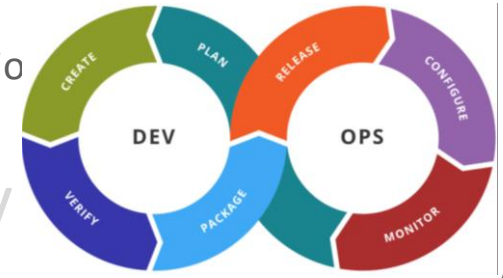
Identity Mgmt
Single Sign-On
Authentication
Governance
Self-Service
Compliance
Access Mgmt
Authorisation

procesy



technológie

IT Compliance
Application and Service Configuratio
API Security



Application and Service Performance
Patching
Audit

dáta

Preventative Controls
Segregation of Duty
Encryption
Data Masking
Key Management

Administrative Controls
Detective Controls

Na koho/čo má vplyv/dopad GDPR
Detaily

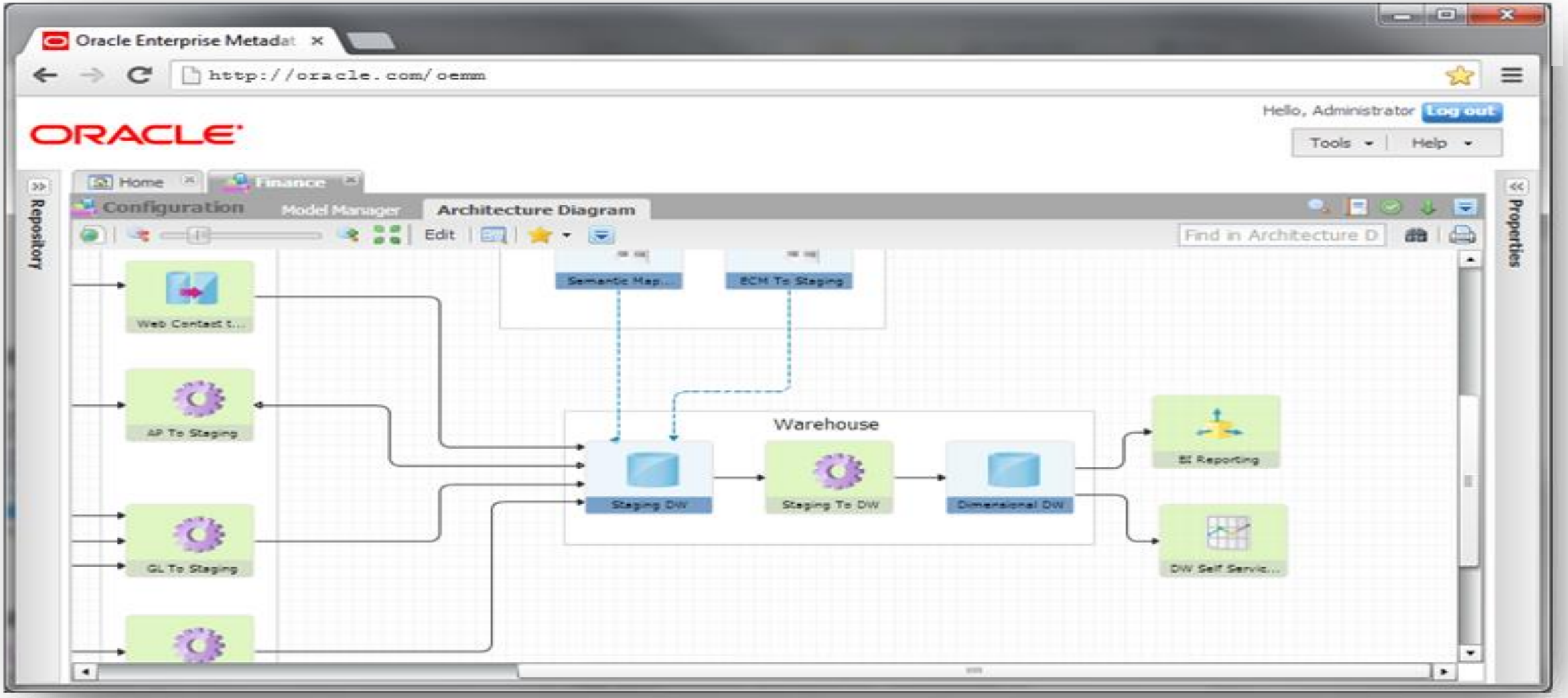
- **ľudia**
  - zamestnanci, zákazníci, dodavatelia, partneri
  - kontinuálne vzdelávanie
  - vyšie povedomie o bezpečnosti
  - nové zodpovednosti
  - zodpovedná osoba
- **procesy**
  - obchodné procesy
  - technologické procesy
  - organizačné opatrenia
  - zmluvné opatrenia
  - kontrola nad spracovaním OÚ
- **technológie**
  - IT infraštruktúra (HW, SW)
  - bezpečnosť „By Design“ a „By Default“
  - vyššie nároky na každej úrovni IT infraštruktúry
  - zavedenie nových technologických opatrení
- **dáta**
  - primeraná úroveň ochrany
  - dôvernosť / dostupnosť / integrita
  - prevencia
  - detekcia
  - kontrolné mechanizmy

IT a GDPR

Ako uchopiť GDPR z pohľadu IT - 4 dimenzie

- Ochrana dát vyžaduje znalosť
  - Kde sú dáta uložené
  - Akému riziku sú dáta vystavené
- Musia / mali by byť naplnené určité požiadavky
  - Modifikáciou aplikácií
  - Využitím spoľahlivej architektúry

Príklad
Vyhľadanie citlivých dát a procesov / Diagram architektúry IS



Príklad
Identifikácia rizika / Výstup z bezpečnostného hodnotenia DB

Database Security Risk Assessment - Highly Confidential

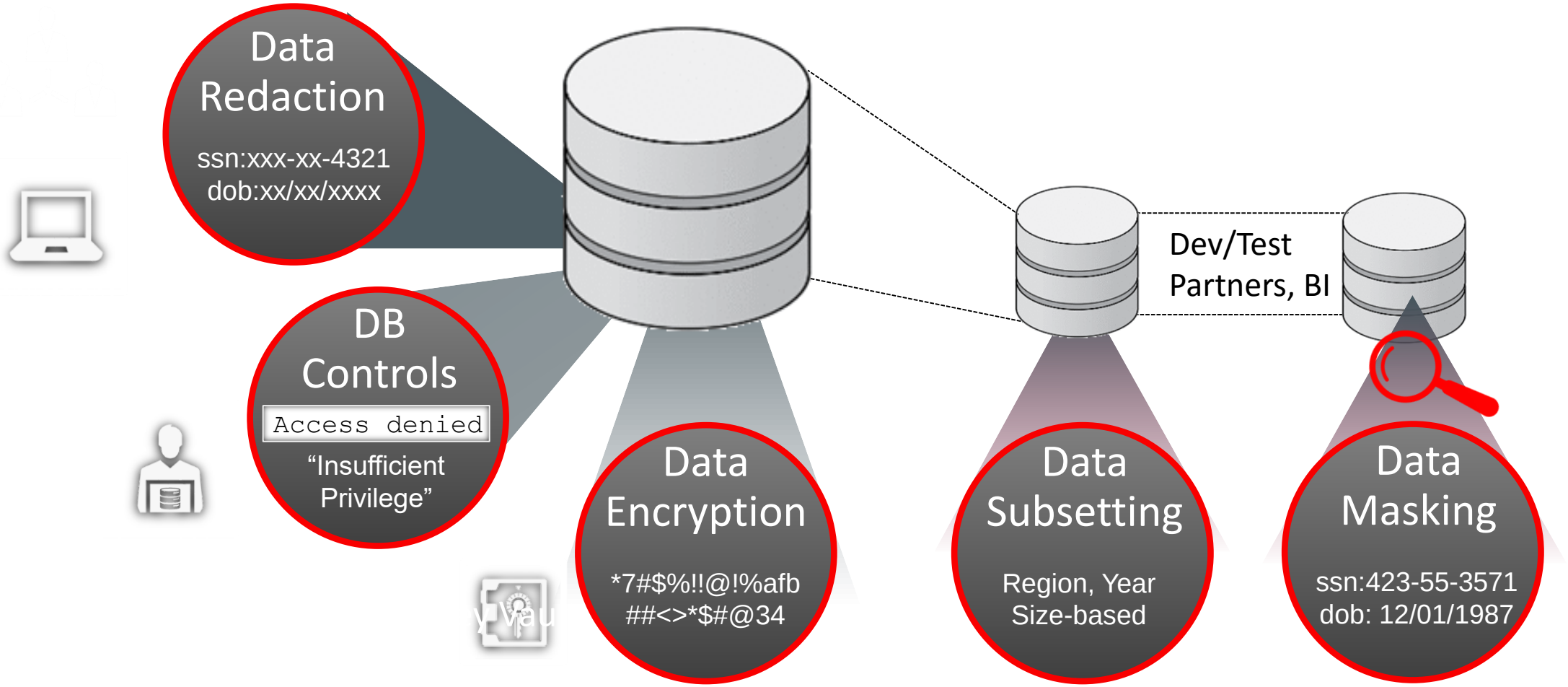
Assessment Date & Time	Date of Data Collection Date of Report Reporter Version ---------- ---------- ---------- Wed Mar 30 2016 13:55:00 Thu Apr 7 2016 12:00:06 0.9 (Apr 2016) - ca6b
Database Identity	Name Platform Database Role Log Mode Created ------ ---------- ---------- ---------- ---------- RDBMS2 Linux x86 64-bit PRIMARY NOARCHIVELOG Wed Mar 30 2016 13:44:00

Basic Information

Item	ID	Status	Result	Remarks
Database Version	Oracle Database 12c Enterprise Edition Release 12.2.0.0.3 - 64bit Production Security options used: Advanced Security, Database Vault, Label Security			
Security Features	Feature Currently Used ---------- ---------- AUTHORIZATION CONTROL Database Vault Yes Privilege Analysis Yes DATA ENCRYPTION Column Encryption Yes Tablespace Encryption Yes Network Encryption No ACCESS CONTROL Data Redaction Yes Virtual Private Database Yes Real Application Security Yes Label Security Yes Transparent Sensitive Data Protection Yes AUDITING Traditional Audit Yes Fine Grained Audit Yes Unified Audit Yes			

Users with Expired Passwords	USER.EXPIRED	Some Risk	Found 1 unlocked user(s) with password expired for more than 30 days.	Password expiration is used to ensure that users change their passwords on a regular basis. If a user's password has been expired for more than 30 days, it indicates that the user has not logged in for at least that long. Accounts that have been unused for an extended period of time should be investigated to determine whether they should remain active.
User Accounts in SYSTEM or SYSAUX Tablespace	USER.TBLSPACE	Significant Risk	40 user(s) use SYSTEM or SYSAUX tablespace.	The SYSTEM and SYSAUX tablespaces are reserved for Oracle-supplied user accounts. To avoid a possible denial of service caused by exhausting these resources, regular user accounts should not use these tablespaces. Prior to Oracle Database 12.2, the SYSTEM tablespace cannot be encrypted, and this is another reason to avoid user schemas in this
Sample Schemas	USER.SAMPLE	Significant Risk	Found 9 sample schema(s).	Sample schemas are well-known accounts provided by Oracle to serve as simple examples for developers. They generally serve no purpose in a production database and should be removed because they unnecessarily increase the attack surface of the
Users with Default Passwords	USER.DEFPWD	Severe Risk	12 unlocked user account(s) are using default password	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.
Password Verifier Version	USER.VERIFIER	Pass	All user accounts have updated password verifiers.	Over time, Oracle releases have added support for increasingly secure algorithms for generating password verifiers for user accounts. In order to remain compatible with older client software, the database continues to generate password verifiers using the previous algorithms as well. Each user account should include a verifier for latest version supported by the database so that the user can be authenticated using the latest algorithm supported by the client. When all clients have been updated, the security of user accounts can be improved by removing the obsolete verifiers.

Príklad
Znižovanie rizika / Architektúra maximálnej bezpečnosti



Cesta k súladu

- Dosiahnutie súladu vyžaduje sadu koordinovaných krokov rôznych oddelení v každej spoločnosti.
- Požaduje pokrytie oblastí:
  - Organizačnej
  - Právnej a zmluvnej
  - Informačných technológií
- Vhodná technológia môže účinne pomôcť súlad s nariadením dosiahnuť

- Oracle poskytuje technológiu, ktorá
  - Zlepšuje dôvernosť, integritu a dostupnosť
  - Zabezpečuje odolnosť systémov spracovania
  - Pomáha pri vyhľadávaní citlivých údajov
  - Zmierňuje bezpečnostné incidenty
- Oracle môže pomôcť začleniť technológiu do správneho kontextu

Oracle UK > About Oracle > Features > General Data Protection Regulation

Oracle security solutions

GDPR is Coming. Are You Ready?

Learn how Oracle Security Solutions can help organizations implement controls that reduce the risk of non-compliance fines around GDPR.

oracle.com/goto/gdpr

Integrated Cloud

Applications & Platform Services