

ORACLE®



GDPR

Analýza rizík,
identifikácia a spravovanie citlivých dát,
implementácia opatrení

Technológie ako účinná pomoc v procese zosúladenia sa s GDPR

Iveta Šťavinová
Oracle
September 2017

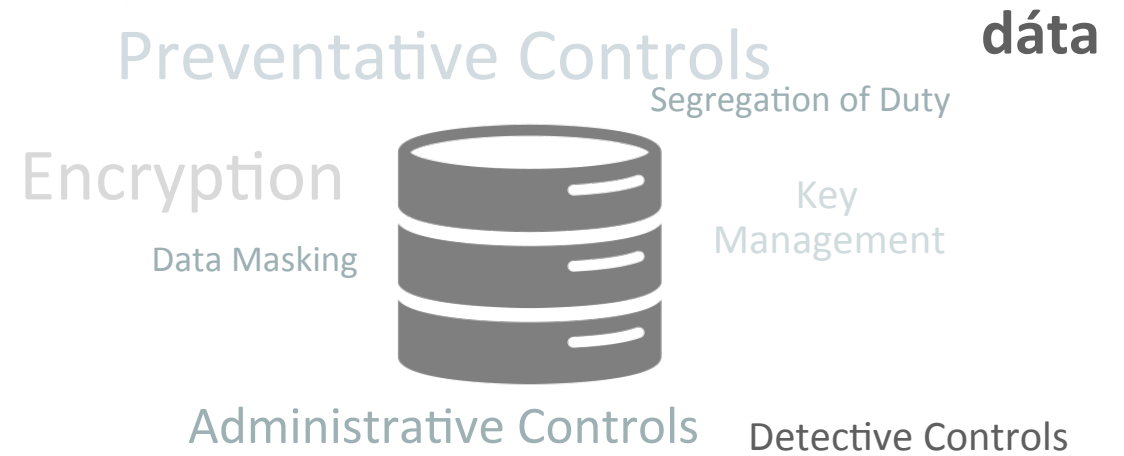
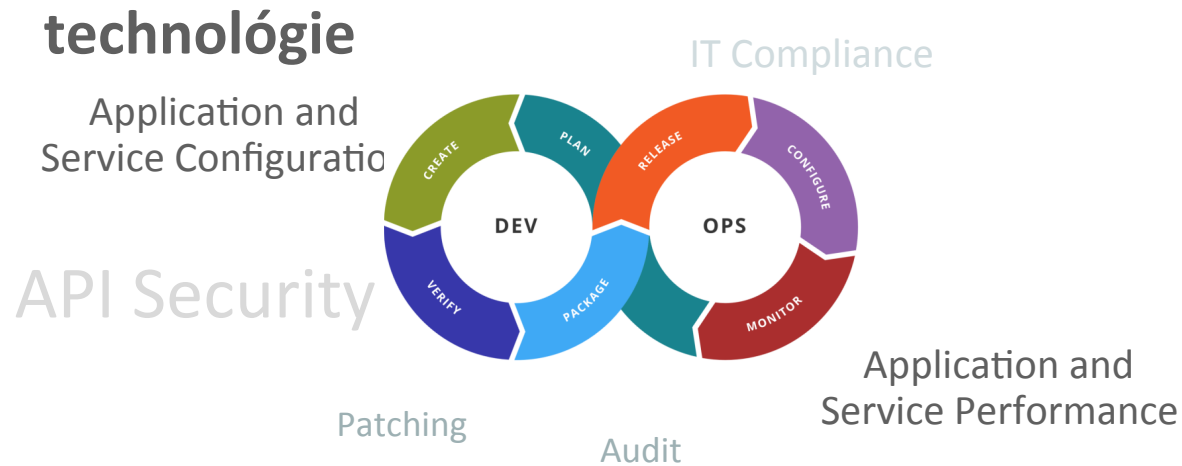
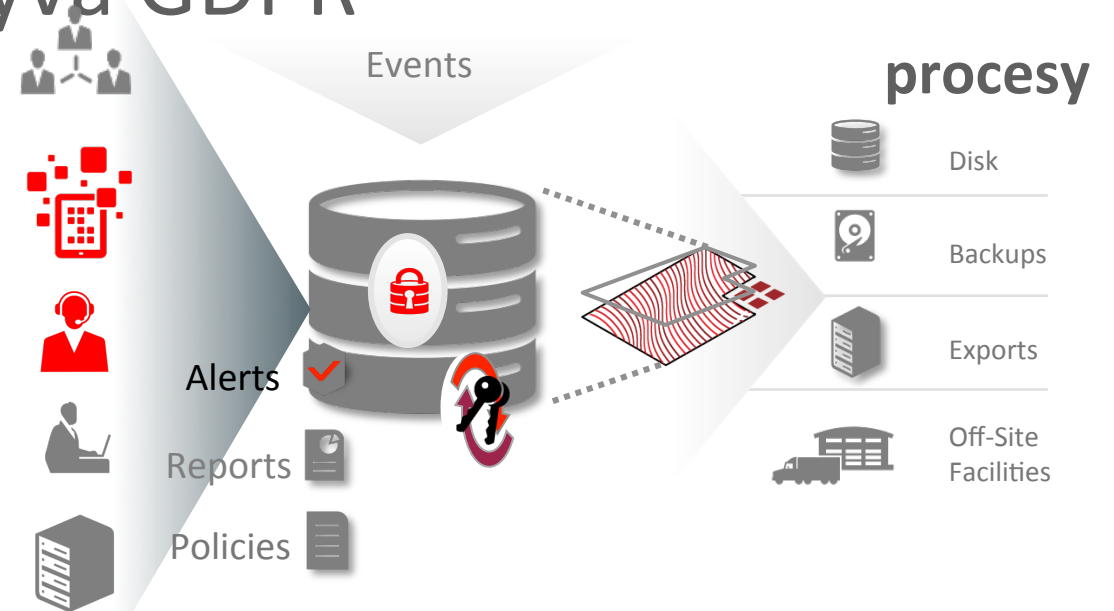
Safe Harbor

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 funkcionality, 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

Štyri hlavné oblasti na ktoré vplýva GDPR



Na koho/čo má vplyv/dopad GDPR

Detaily

- **ľudia**

- zamestnanci, zákazníci, dodavatelia, partneri
- kontinuálne vzdelávanie
- vyšie povedomie o bezpečnosti
- nové zodpovednosti
- zodpovedná osoba

- **technológie**

- IT infraštruktúra (HW, SW)
- bezpečnosť „By Design“ a „By Default“
- vyššie nároky na každej úrovni IT infraštruktúry
- zavedenie nových technologických opatrení

- **procesy**

- obchodné procesy
- technologické procesy
- organizačné opatrenia
- zmluvné opatrenia
- kontrola nad spracovaním OÚ

- **dáta**

- primeraná úroveň ochrany
- dôvernosc' / 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



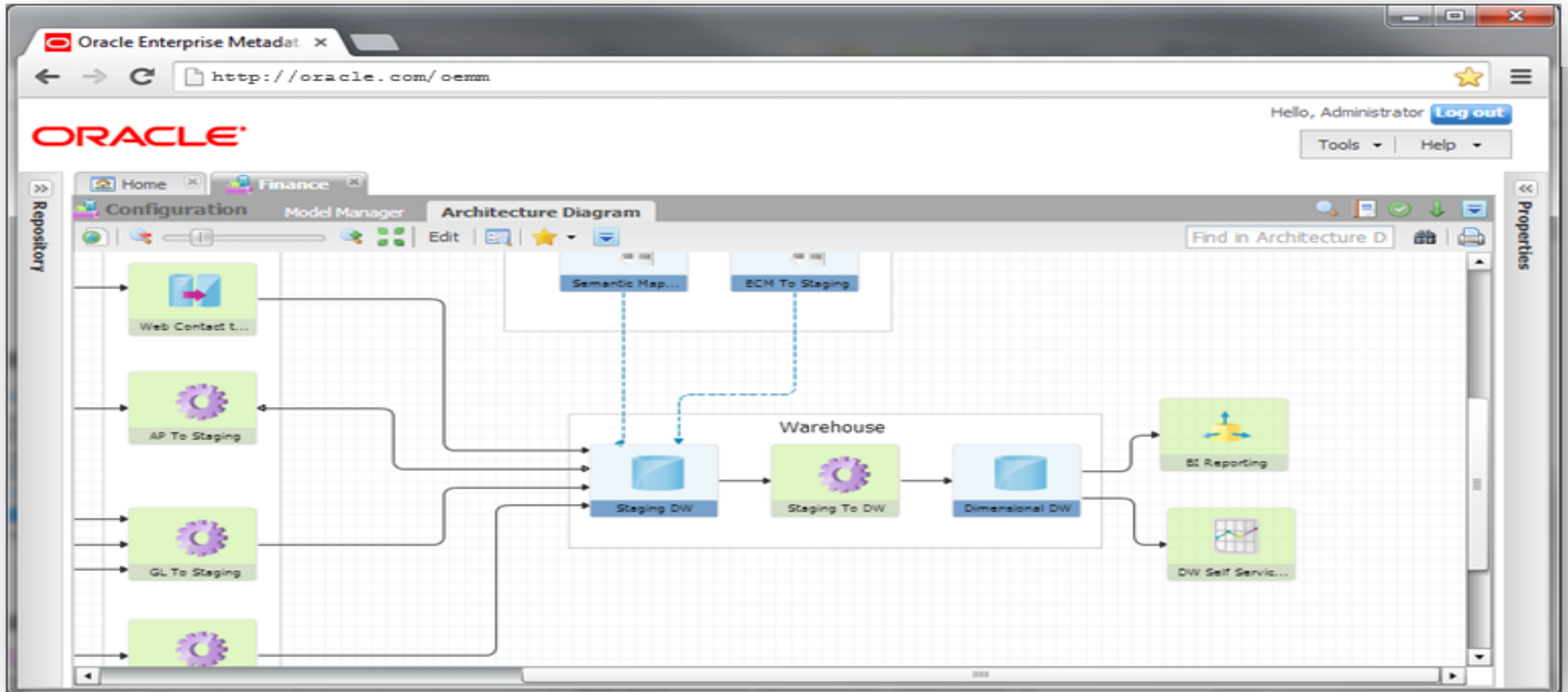
Dáta / Záznamy o spracovaní

Každý prevádzkovateľ a v príslušnom prípade zástupca prevádzkovateľa vedie záznamy o spracovateľských činnostiach, za ktoré zodpovedá (*Článok 30*)

- info o prevádzkovateľovi, účel spracúvania, kategórie osôb a osobných údajov, info o prenosoch, lehoty na vymazanie, opis implementovaných bezp. opatrení....
- sprostredkovateľ vedie záznamy v rovnakom rozsahu ako prevádzkovateľ
- písomne / elektronicky
- sprístupnenie záznamov dozornému orgánu
- **Identifikácia IS** – ktoré systémy, spôsob spracovania
- **Vyhľadanie dát** - veľa rôznych formátov, umiestnení a typov dát
- Identifikácia a **riadenie dátových tokov**
- Identifikácia dát a ich **prilinkovanie k procesom**
- Budovanie glosára kritických dát
- **Vytvorenie pravidiel**, kontrola dátového toku, kontrola zdieľania dát, kontrola vymazania
- **Jednotný pohľad** na dotknutú osobu - schopnosť re-lokalizovať relevantné dáta

Enterprise Metadata Manager, Data Quality, Data Integrator

Príklad Diagram architektúry IS



Posúdenie rizík a vplyvu na ochranu údajov

POCHOPENIE RIZIKA

Spoločnosti musia pochopiť a znížiť riziká pre dotknutú osobu



Prevádzkovateľ aj sprostredkovateľ musia pochopiť a redukovať riziká pre dotknutú osobu

- (DPIA) Posúdenie vplyvu na ochranu osobných údajov (Článok 35)
 - posúdenie rizika pre práva a slobody dotknutých osob
 - opatrenia na riešenie rizík
 - prehodnotenie ak došlo k zmene rizika
 - konzultácia a získanie súhlasu dozorného orgánu ak je to nevyhnutné
- Referencovanie štandardov, resp. postup podľa noriem pre riadenie rizík
 - ISO 31000:2009, Risk management — Principles and guidelines, and ISO/IEC 29134 (project), Information technology – Security techniques – Privacy impact assessment – Guidelines
- Automatizácia procesu hodnotenia rizika
- Podpora hodnotenia bezp. opatrení
- Reporting

Database Security Assessment Tool, Security Assessment & Roadmap Service

Príklad

Výstup z bezpečnostného hodnotenia DB vo formáte .xls

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.VERIFYR	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.



Práva dotknutej osoby

Kapitola 3 “Práva dotknutej osoby” (Oddiel 2 a 3) poskytuje zoznam povinností prevádzkovateľa

- Právo dotknutej osoby na prístup k údajom (Článok 15)
- Právo na opravu (Článok 16)
- Právo na vymazanie (právo ‘na zabudnutie’) (Článok 17)
- Právo na obmedzenie spracovávania (Článok 18)
- Oznamovacia povinnosť v súvislosti s opravou alebo vymazaním osobných údajov alebo obmedzením spracúvania (Článok 19)
- Právo na prenosnosť údajov (Článok 20)
- Manuálny zásah človeka
 - Váhovanie požiadaviek nariadenia a ďalších zákonov - vymazanie sa vyhodnotí s prihliadnutím na zákony a práva iných subjektov
- Portabilita dát (modifikácia aplikácie)
 - Prenosnosť údajov požadovaná subjektom vyžaduje funkciu na export vo formáte čitateľnom strojom (machine-readable format)

Project management, Change management



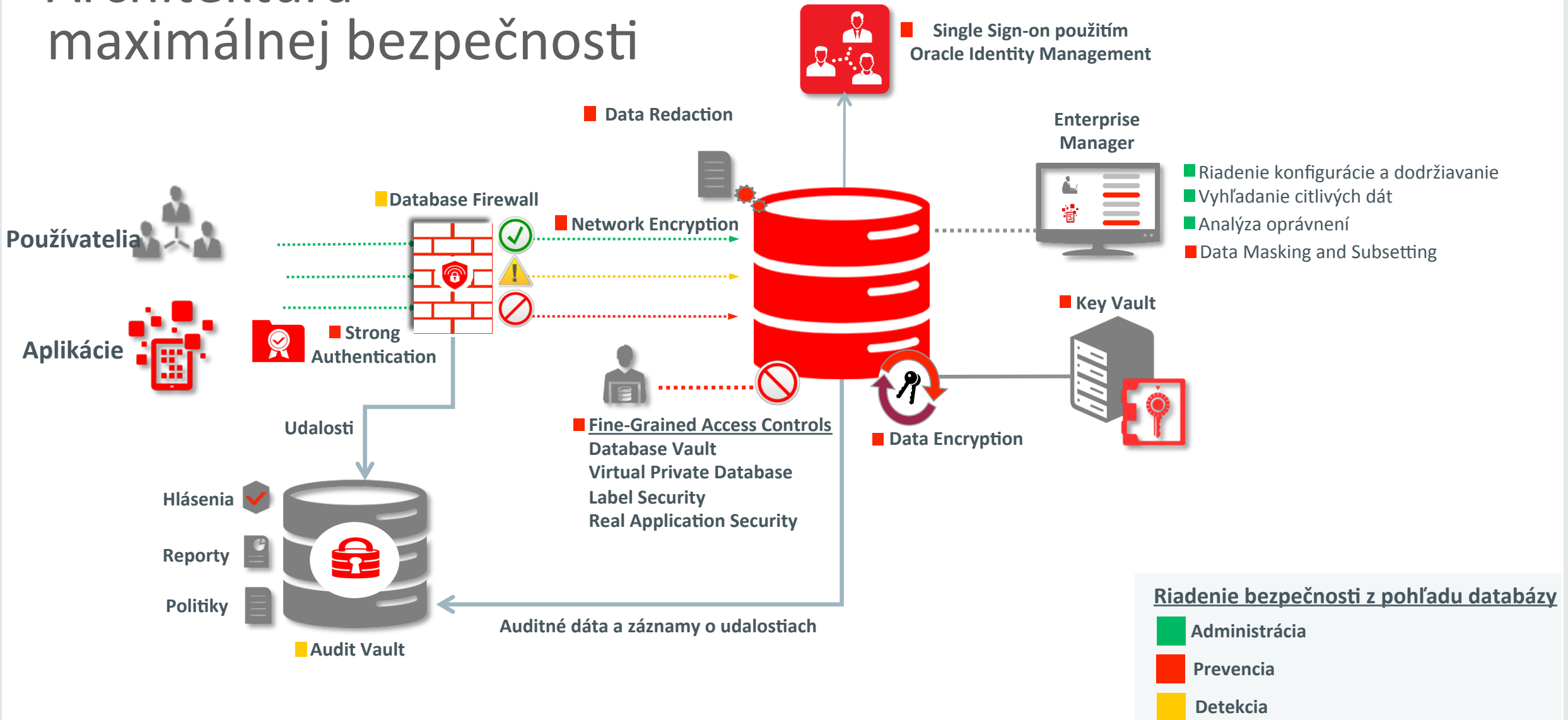
Bezpečnostné opatrenia

Niektoré články referencujú povinnosť, resp. úlohu prijať **primerané technické a organizačné opatrenia**

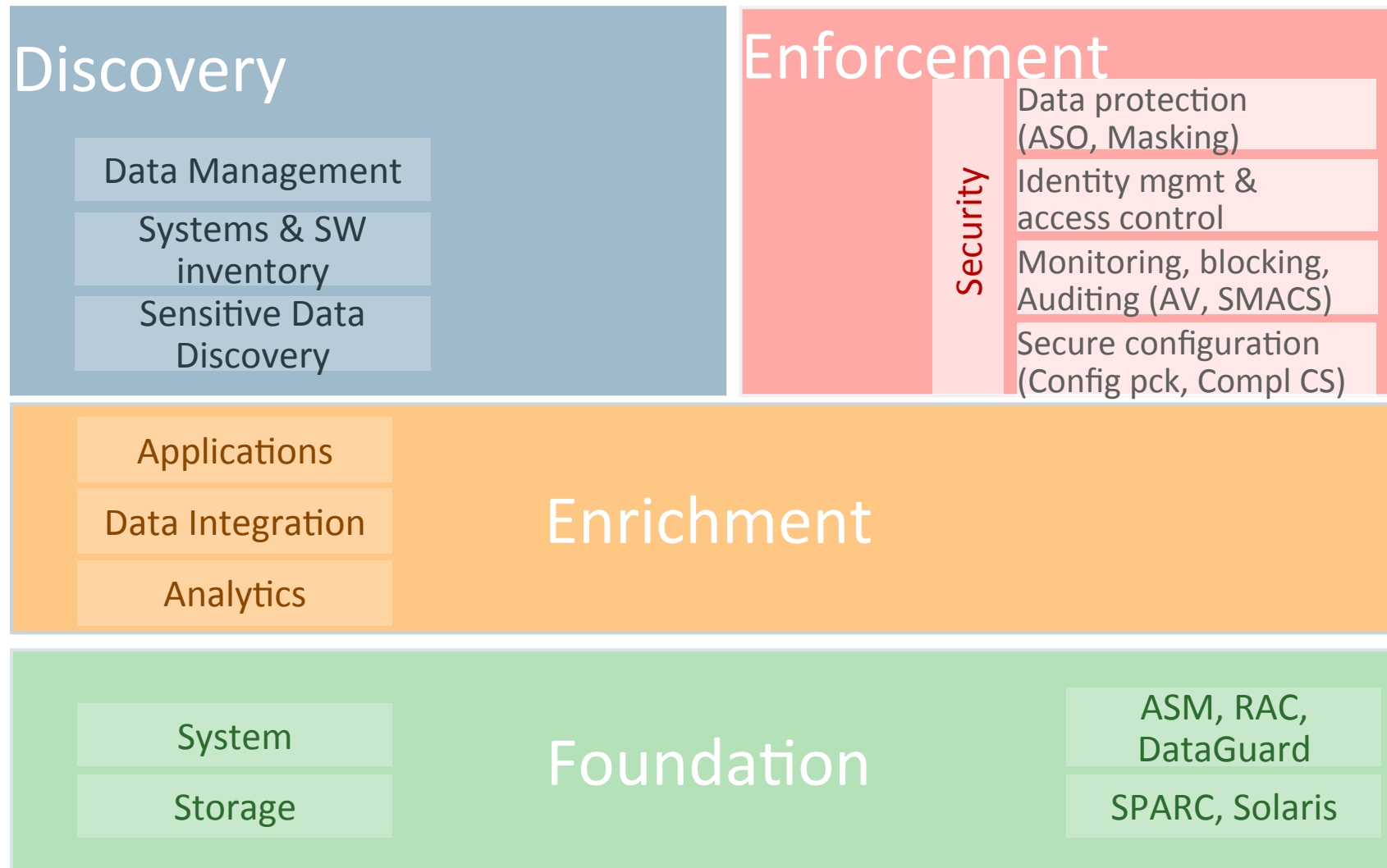
- Zásady spracúvania osobných údajov (Článok 5)
- Zodpovednosť prevádzkovateľa (Článok 24)
- Špecificky navrhnutá a štandardná ochrana údajov (Článok 25)
- Sprostredkovateľ (Článok 28)
- Bezpečnosť spracúvania (Článok 32)
- Oznámenie porušenia ochrany osobných údajov dotknutej osobe (Článok 34)
- Šifrovanie, anonymizácia, pseudonymizácia
- Autentifikácia, autorizácia, riadenie prístupu k dátam
- Zabránenie úniku dát, kontrola integrity
- Riešenia pre vysokú dostupnosť, záložné sídlo, archivácia
- Monitoring
- Technológie a postupy rýchlej obnovy

Advanced Security, Redaction, DB Vault, Masking, IdM, RAC, DataGuard, OEM, SOC (Compliance, Change & Config, Reporting, SMA)

Architektúra maximálnej bezpečnosti



Cesta k súladu



Oracle produkty, alebo Cloud služby môžu pomôcť pri ceste k súladu s GDPR.

Možnosť pomôcť:

- 1. Vyhládať** citlivé dáta použitím riešení pre data governance (správovanie dát)
- 2. Vynucovať/implementovať bezpečnostné opatrenia** pre dáta, software a identity
- 3. Obohatiť** aplikačné funkcie tak, aby bolo možné garantovať práva dotknutých subjektov
- 4. Podporovať základ**, ktorý zahŕňa správne IT praktiky, vysokú dostupnosť a odolnosť IT

GDPR & Oracle

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

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



Live Webcast

Accelerate EU GDPR
Compliance with
Database Security, June
27, 2017



On-demand Webcast

How Selected Oracle
Data Security Solutions
May Assist with Your
GDPR Compliance



Whitepaper

Accelerate Your
Response to the EU
General Data Protection
Regulation (GDPR)

Accelerate Your Response to the EU General Data Protection Regulation (GDPR)
Using Oracle Database Security Products



Integrated Cloud

Applications & Platform Services

ORACLE®