Oracle Database Security

eakce na požadavky EU GDPR

roslav Novotný
Architect

ORACLE

Disclaimer

The information in this document may not be construed or used as legal advice about the content, interpretation or application of any law, regulation or regulatory guideline. Customers and prospective customers must seek their own legal counsel to understand the applicability of any law or regulation on their processing of personal data, including through the use of any vendor's products or services.

Současný stav ochrany dat v EU

- Dvě desetiletí stará směrnice o ochraně údajů 95/46/EC
- Roztříštěný způsob provádění vzhledem k rozdílnému výkladu v jednotlivých zemích
- Zastaralé vzhledem k rychlému technologickému rozvoji a globalizaci
- Slabá reakce na zvýšený počet bezpečnostních incidentů

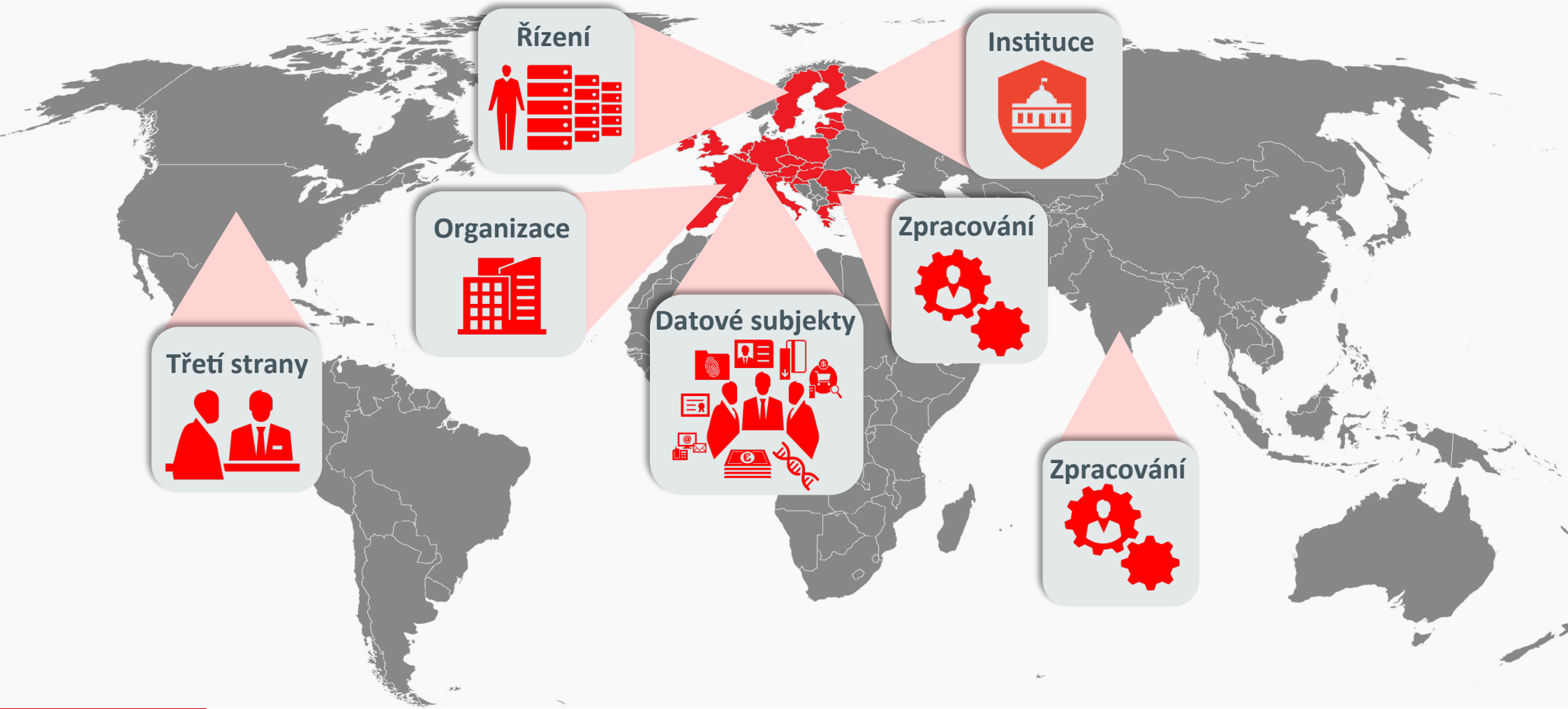
ORACLE

General Data Protection Regulation (GDPR)

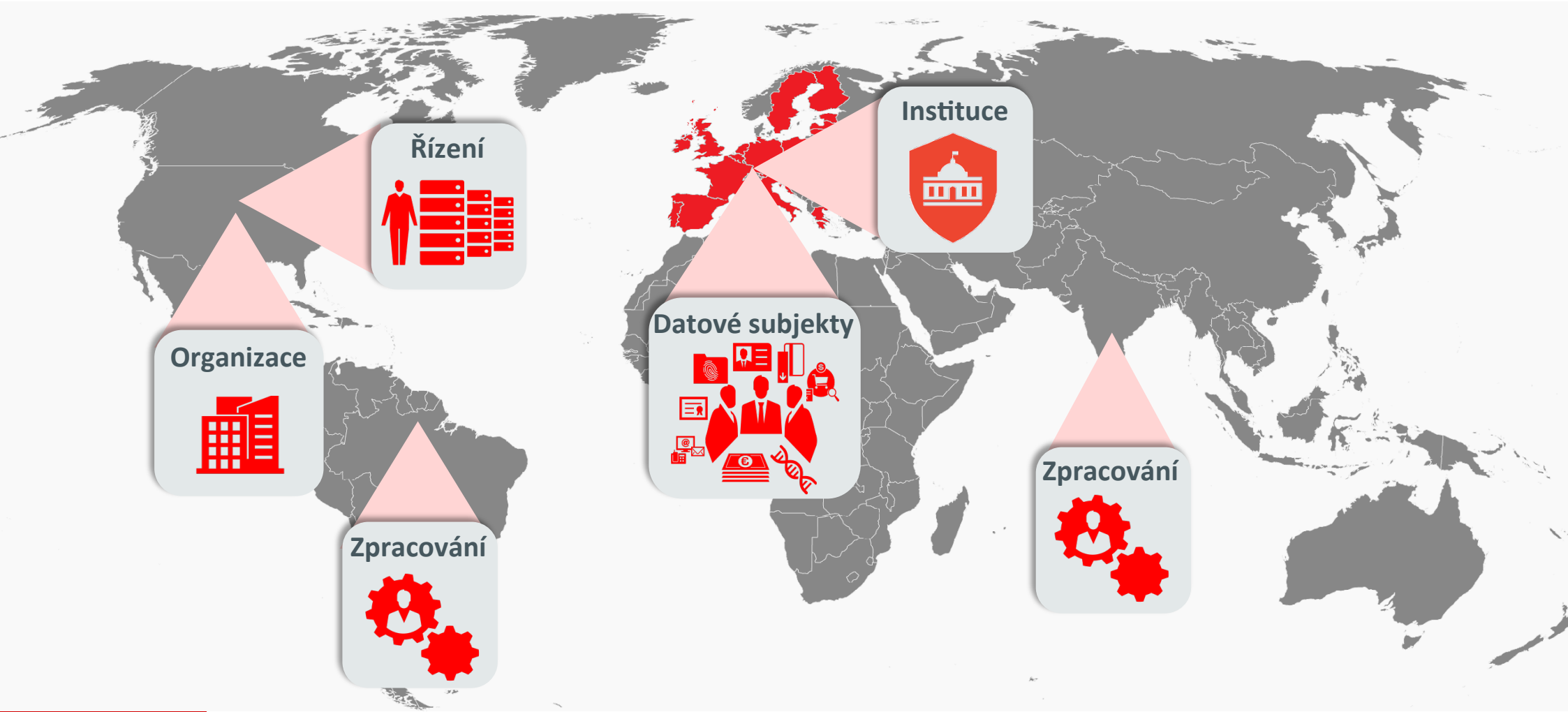
lavní cíle

- Definovat základní úroveň ochrany údajů
- Vyjasnit odpovědnost za ochranu údajů
- Vypracovat v souladu s principy ochrany osobních údajů
- Reagovat na technologické změny
- Umožnit volný tok dat
- Zajistit prosazení – regulace vs direktiva

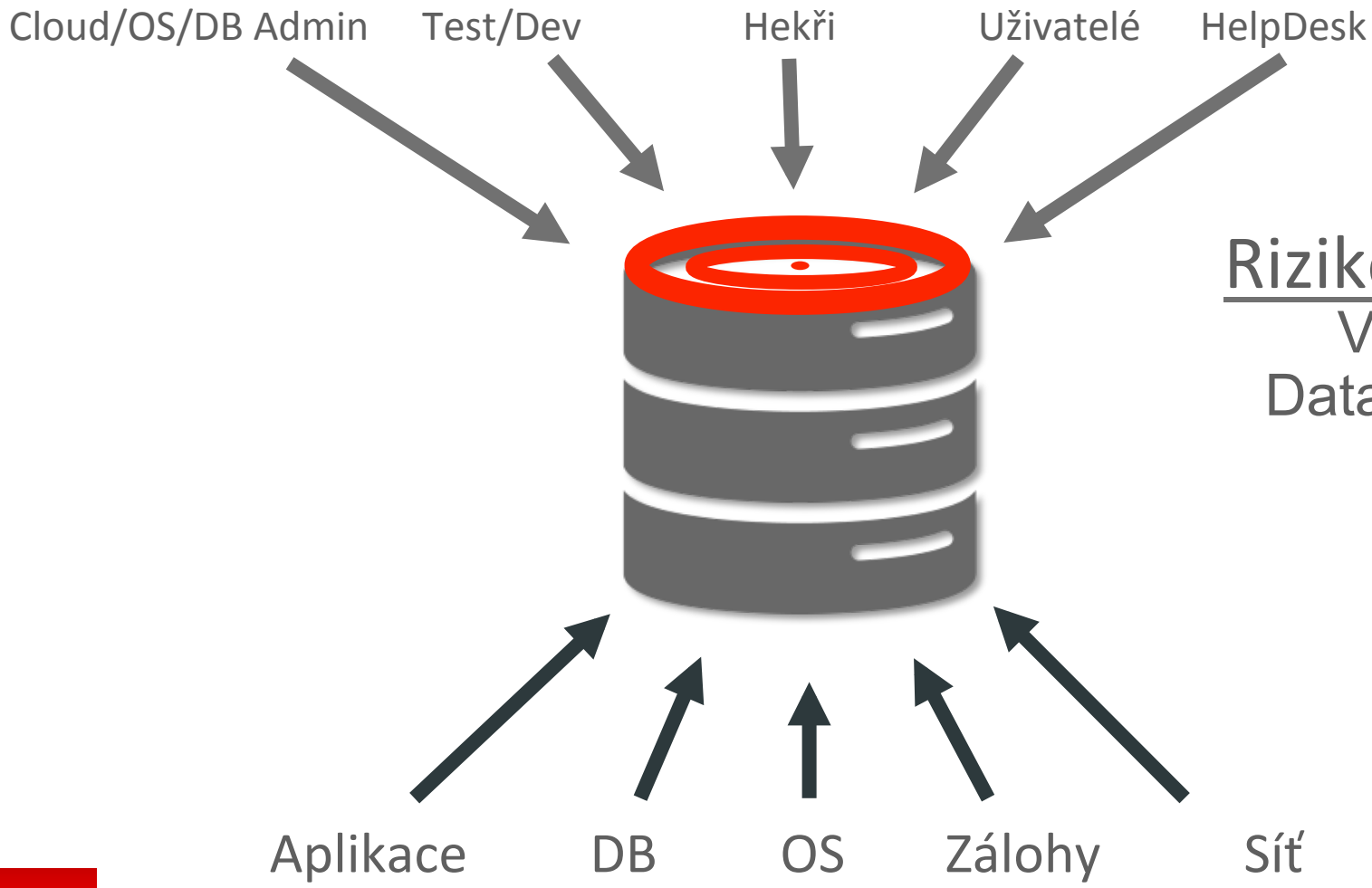
Hlavní aktéři GDPR



Hlavní aktéři GDPR *(mimo EU – pokračování)*



Hrozby – Aktéři, Původci a Cíle



Rizikové multiplikáto
Vysoká dostupnost
Databázová konsolidac
Starší aplikace
Outsourcing
Cloud

GDPR Klíčové Bezpečnostní Principy

POSOUDIT	CHRÁNIT	ODHALIT
Procesy, Profily, Citlivost dat, Rizika	Šifrování, Pseudonymizace, Anonymizace, Detailní řízení přístupu, Řízení privilegovaných přístupů, Oddělení rolí	Audit, Monitorování aktivit, Upozorňování, Reportování

ORACLE

Posouzení bezpečnostních rizik

http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R067

Odkaz	GDPR znění	Řízení bezpečnosti z pohledu Oracle Database
lánek 35	…Provede správce před zpracováním **posouzení vlivu zamýšlených operací** zpracování na ochranu osobních údajů…	• Použití **Oracle Enterprise Manager's Database Lifecycle Management Pack** pro posouzení zabezpečeného profilu Oracle Databases zkoumáním její konfigurace. • Použití **Oracle Enterprise Manager's Application Data Modeling** pro posouzení všech dostupných citlivých údajů prozkoumáním databázových sloupců s citlivými informacemi. • Použití **Oracle Database Vault Privilege Analysis** pro posouzení, k jakým citlivým údajům se přistupuje průzkumem rolí a oprávnění v Oracle Database. • Použití **Oracle Security Assessment Tool** pro vyhodnocení konfigurace databáze z pohledu zabezpečení, nastavení bezpečnostních politik, stavu uživatelů, rolí a oprávnění.
itace 84	… v případech, kdy je pravděpodobné, že operace zpracování budou představovat vysoké riziko pro práva a svobody fyzických osob, by měl být **správce odpovědný za provedení posouzení** vlivu na ochranu osobních údajů, aby vyhodnotil zejména původ, povahu, zvláštnost a závažnost tohoto rizika…	
itace 91	… **Posouzení vlivu na ochranu osobních údajů** je rovněž zapotřebí v případě monitorování veřejně přístupných prostor prováděného ve velkém rozsahu …	

Nalezení citlivých dat

Průzkum konfigurace z pohledu bezpečnosti

Analýza rolí a oprávnění

Ochrana proti útokům

http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R067

Odkaz	GDPR znění	Řízení bezpečnosti z pohledu Oracle Database
Článek 32	… provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně: … …**pseudonymizace a šifrování osobních údajů;** …	• Použití **Oracle Advanced Security - Transparent Data Encryption** pro šifrování dat. • Použití **Oracle Advanced Security - Data Redactio** pro pseudonymizaci dat u produkčních aplikacích. • Použití **Oracle Data Masking and Subsetting** pro anonymizaci dat u ne-produkčních aplikací.
Citace 83	V zájmu zachování bezpečnosti a zabránění zpracování, které by bylo v rozporu s tímto nařízením, by měl správce nebo zpracovatel posoudit rizika spojená se zpracováním a přijmout opatření ke zmírnění těchto rizik, například **šifrování** …	
Citace 28	Použití **pseudonymizace** osobních údajů může omezit rizika pro dotčené subjekty údajů a napomoci správcům a zpracovatelům splnit jejich povinnosti týkající se ochrany údajů.	

Ochrana proti útokům *(pokračování)*

http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R067

Odkaz	GDPR znění	Řízení bezpečnosti z pohledu Oracle Database
itace 26	Zásady ochrany osobních údajů by se proto neměly vztahovat na **anonymní informace, totiž informace, které se netýkají identifikované či identifikovatelné fyzické osoby, ani na osobní údaje anonymizované tak, že subjekt údajů není nebo již přestal být identifikovatelným**….	• Použití **Oracle Data Masking and Subsetting** pro maskování či anonymizaci dat v ne-produkčním prostředí.
lánek 5	Osobní údaje musí být: přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („**minimalizace údajů**“);	• Použití **Oracle Data Masking and Subsetting** pro vytvoření podmnožiny dat, odstraněním či vytažením části dat na jiné umístění.
lánek 20	Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, **a právo předat tyto údaje jinému správci** …	

Ochrana proti útokům *(pokračování)*

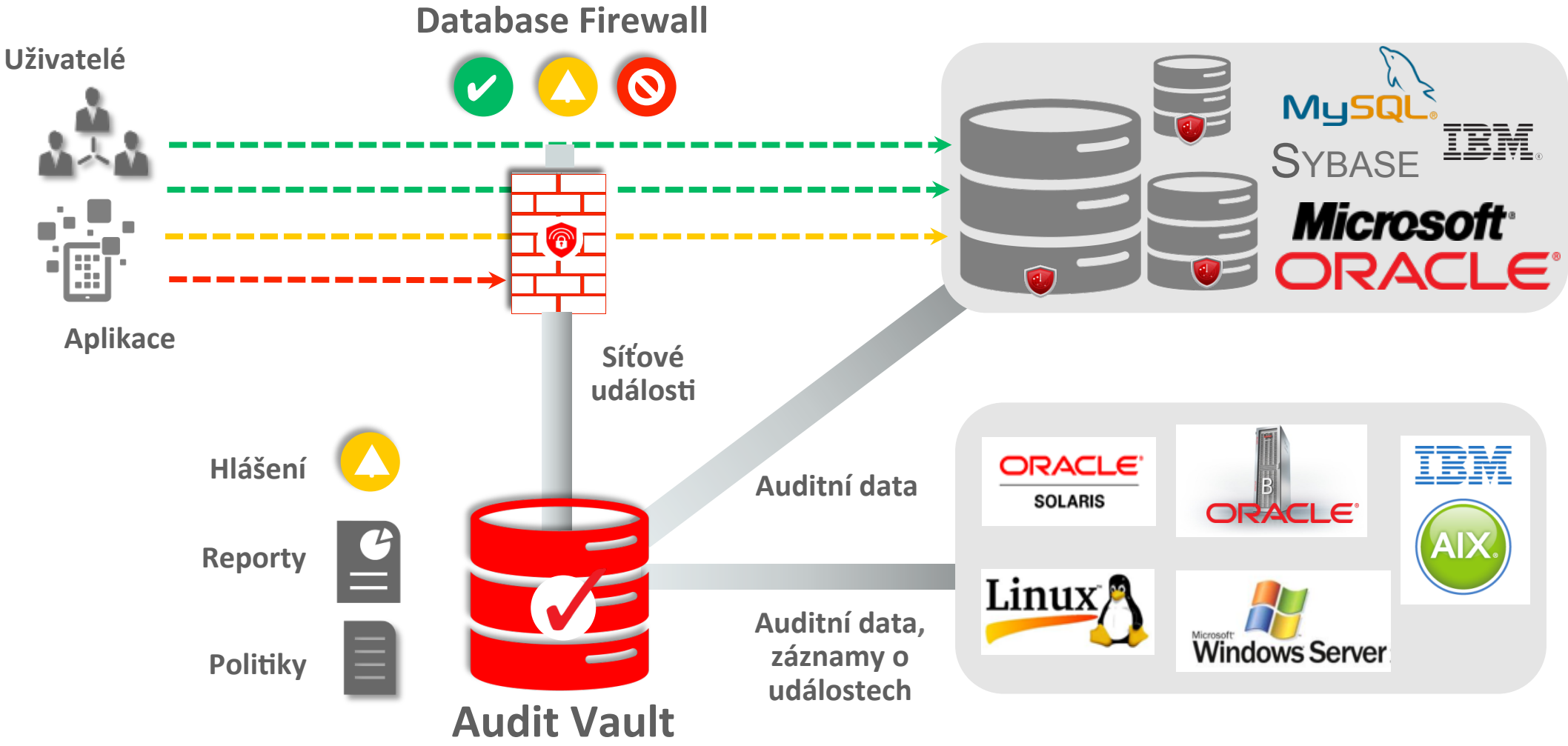
http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R067

Odkaz	GDPR znění	Řízení bezpečnosti z pohledu Oracle Database
Článek 29	**Zpracovatel a jakákoliv osoba, která jedná z pověření správce** nebo zpracovatele a má přístup k osobním údajům, **může tyto osobní údaje zpracovávat pouze na pokyn správce** …	• Použití **Oracle Virtual Private Database** pro detailní řízení přístupu k údajům • Použití **Oracle Label Security** pro klasifikaci a označení údajů podle citlivosti obsažené informac • Použití **Oracle Label Security** pro řízení přístupu n základě klasifikace údajů • Použití **Oracle Database Vault** pro řízení přístupu privilegovaných uživatelů, kteří zpracovávají data.
Článek 32	4) Správce a zpracovatel přijmou opatření pro zajištění toho, aby **jakákoliv fyzická osoba, která jedná z pověření správce nebo zpracovatele a má přístup k osobním údajům, zpracovávala tyto osobní údaje pouze na pokyn správce** …	
Citace 64	Správce by měl využít všech vhodných opatření k **ověření identity subjektu údajů, který žádá o přístup**, zejména v souvislosti s on-line službami a síťovými identifikátory…	• Použití metod **Oracle Strong Authentication** jako např. SSL nebo Kerberos spolu s **Real Application Security (RAS)** pro ověření identity databáze a aplikačních uživatelů přistupujících k citlivým údajům.

Monitorování za účelem **odhalení hrozby**

http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R067

Odkaz	GDPR znění	Řízení bezpečnosti z pohledu Oracle Database
lánek 30	Každý správce a jeho případný zástupce vede **záznamy o činnostech zpracování**, za něž odpovídá. …	• Použití **Oracle Database Auditing** pro sledování a údržbu záznamů (auditních záznamů) během prác s daty. • Použití **Oracle Fine Grained Auditing** pro záznam a audit specifických aktivit uživatelů jako např. výbě citlivých dat apod. • Použití **Oracle Audit Vault and Database Firewall** pro centrální řízení záznamů o aktivitách a zpracování dat. • Použití **Oracle Audit Vault and Database Firewall** pro monitorování a zasílání upozornění na podezřelé chování.
itace 82	Aby správce nebo zpracovatel doložil soulad s tímto nařízením, měl by vést **záznamy o činnostech zpracování**, za které odpovídá. …	
lánek 33	Jakékoli **porušení zabezpečení osobních údajů** správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, **ohlásí** dozorovému úřadu ...	



Kvalita ochrany

CENTRALIZOVANÁ

ADMINISTRACE

KONTROLA

SBĚR

OPRÁVNĚNÍ

- Použít **Oracle Key Vault** pro centrální řízení klíčů při práci s osobními údaji
- Použít **Oracle Audit Vault and Database Firewall to** pro centrální sběr a řízení auditních záznamů

Kvalita ochrany *(pokračování)*

http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R067

Odkaz	GDPR znění	Oracle Database Security Control
Článek 25	…zavede správce **jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření**, jako je pseudonymizace, jejichž účelem je provádět zásady ochrany údajů, jako je minimalizace údajů, účinným způsobem a začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů.	• Použití **Oracle Database Security maximum security architecture** pro ochranu dat, jak uvnitř databáze, tak příchozích dat, dále pak návrh nasazení řídících prvků do architektury, sloužících pro posouzení citlivých dat, návrh preventivních ochran a v neposlední řadě návrh detektivních činností, když je nutné identifikovat původce zneužití údajů.
Článek 32	Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména **náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.**	

Řízení bezpečnosti z pohledu Oracle

ADMINISTRACE	PREVENCE	DETEKCE
Bezpečná konfigurace	Šifrování a redakce	Audit
Nalezení citlivých dat	Maskování a menší množina dat	Monitorování aktivit
Použití minimálních oprávnění	DBA a řízení provozu	Upozornění a reporty

ORACLE

ORACLE

ORACLE

SYBASE

MySQ

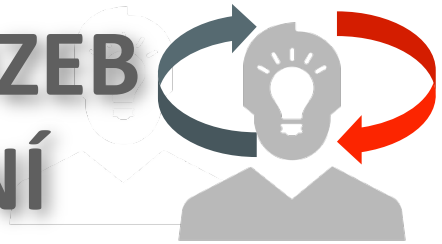
IBM

Micros

ORACLE

Stabilní strategie pro bezpečnost Oracle Database

PŘEDVÍDÁNÍ HROZEB A JEJICH ZMÍRNĚNÍ



ransparent Data Encryption, DBA Control, Redaction, Masking, Privilege Analysis, DB Firewall, RAS, Cloud, …

SECURITY INSIDE-OUT

Zabezpečení, které je, co nejblíže datům: Eliminuje dohady, maximalizuje výkon a je transparentní pro aplikace

DEFENSE-IN-DEPTH SECURITY CONTROLS

řekrývající se prvky: Šifrování, maskování, audit, monitorování, řízení přístupu, redakce, …

ZKUŠENOST S NASAZENÍM

Napříč různými systémy: Operační systémy, heterogenní databáze, aplikace, …

/OracleDatabase

/OracleSecurity

blogs.oracle.com/SecurityInsideOut

blogs.oracle.com/datamasking

Oracle Database Insider

/Oracle/database

/OracleLearning

oracle.com/database/security
oracle.com/technetwork/database/security

Integrated Cloud

Applications & Platform Services