

# Oracle Database Security

## Reakce na požadavky EU GDPR

Jaroslav Novotný  
IT Architect

# 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

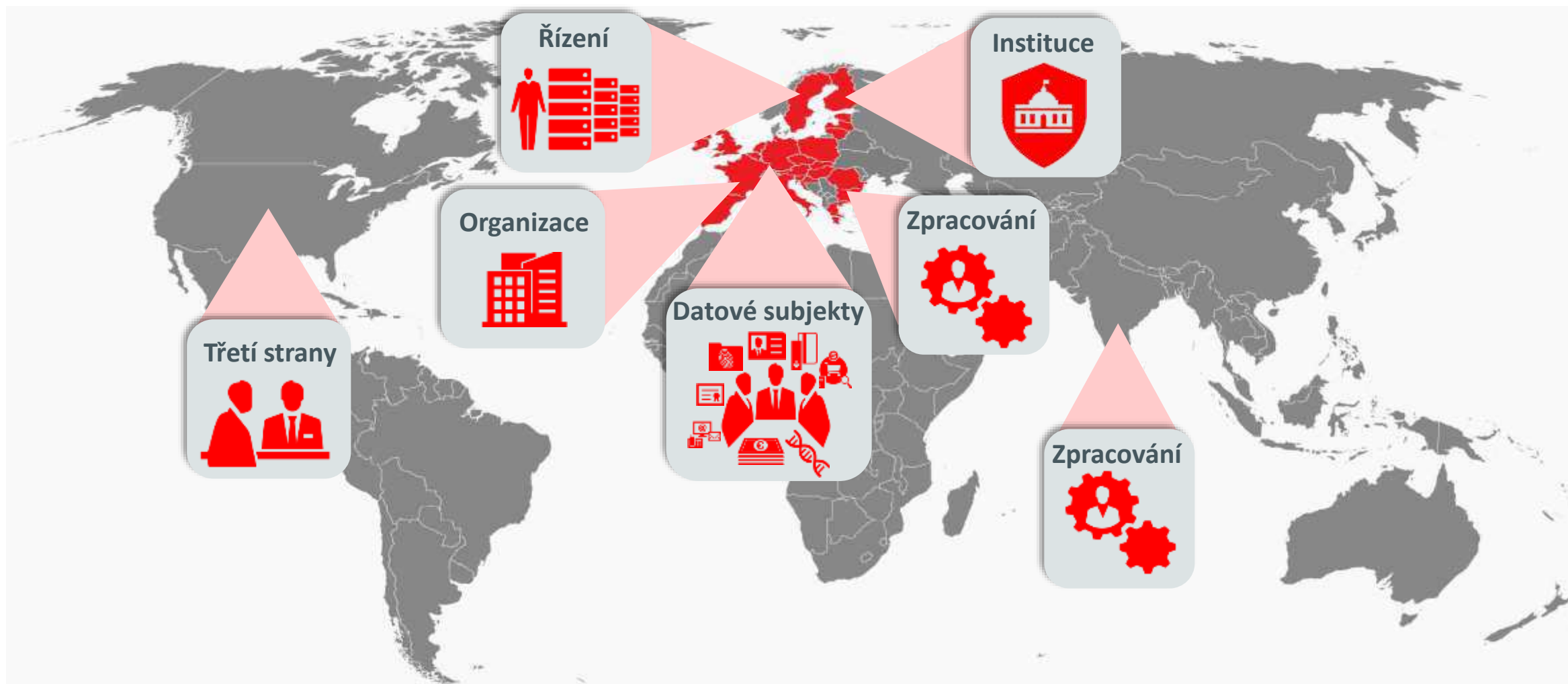
# General Data Protection Regulation (GDPR)

## Hlavní cíle

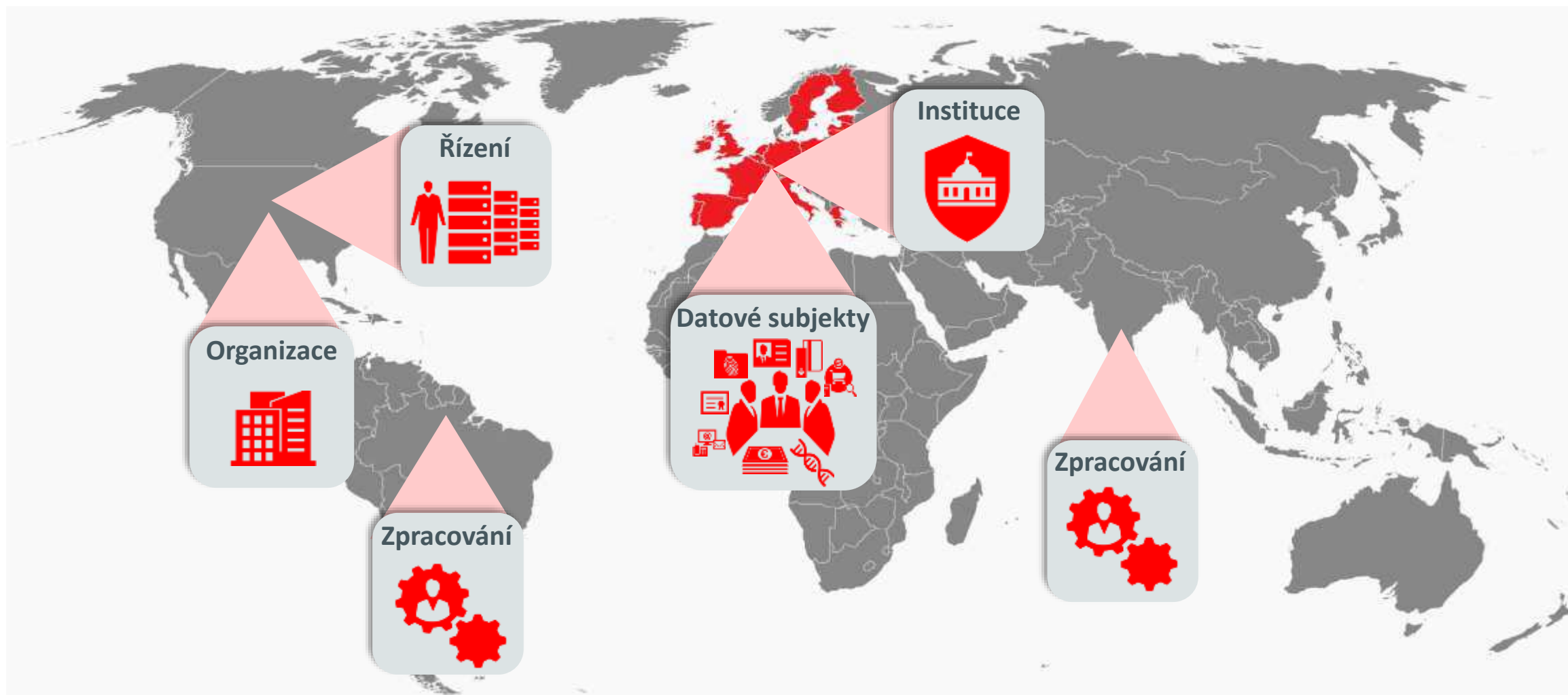
- Definovat základní úroveň ochrany údajů
- Vyjasnit odpovědnost za ochranu údajů
- Vypracovat v souladu s principy ochrany osobních údajů
- Reagovat na technologické změny
- Umožnit volný tok dat
- Zajistit prosazení – regulace vs direktiva



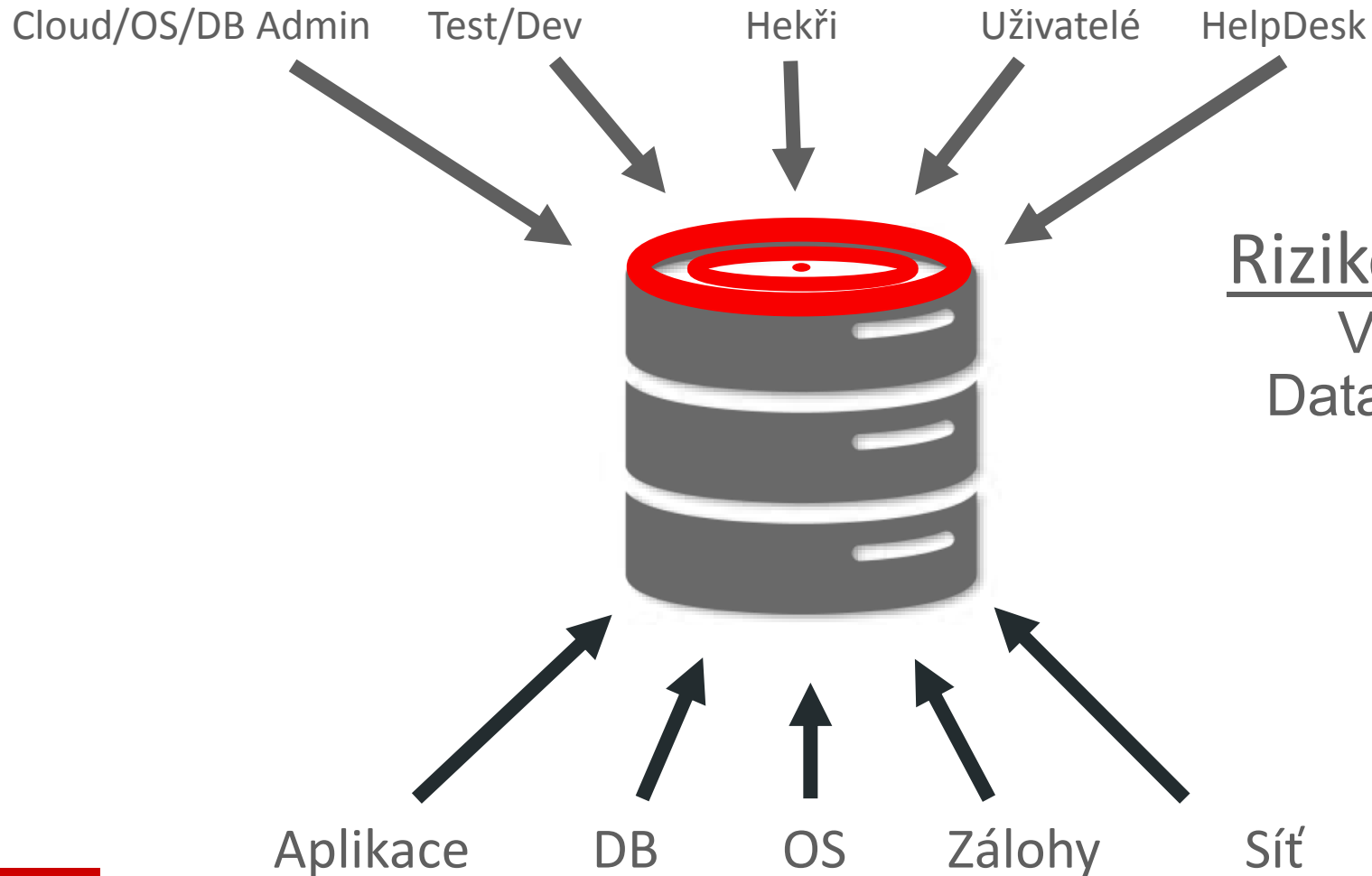
# Hlavní aktéři GDPR



# Hlavní aktéři GDPR *(mimo EU – pokračování)*



# Hrozby – Aktéři, Původci a Cíle



## Rizikové multiplikátory

Vysoká dostupnost  
Databázová konsolidace  
Starší aplikace  
Outsourcing  
Cloud

# GDPR Klíčové Bezpečnostní Principy

## POSOUDIT

Procesy,  
Profily,  
Citlivost dat,  
Rizika

## CHRÁNIT

Šifrování,  
Pseudonymizace,  
Anonymizace,  
Detailní řízení přístupu,  
Řízení privilegovaných  
přístupů,  
Oddělení rolí

## ODHALIT

Audit,  
Monitorování aktivit,  
Upozorňování,  
Reportování



# Posouzení bezpečnostních rizik

<http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0679>

Odkaz	GDPR znění	Řízení bezpečnosti z pohledu Oracle Database
Článek 35	...Provede správce před zpracováním <b>posouzení vlivu zamýšlených operací</b> zpracování na ochranu osobních údajů...	<ul style="list-style-type: none"><li>• Použití <b>Oracle Enterprise Manager's Database Lifecycle Management Pack</b> pro posouzení zabezpečeného profilu Oracle Databases zkoumáním její konfigurace.</li><li>• Použití <b>Oracle Enterprise Manager's Application Data Modeling</b> pro posouzení všech dostupných citlivých údajů prozkoumáním databázových sloupců s citlivými informacemi.</li><li>• Použití <b>Oracle Database Vault Privilege Analysis</b> pro posouzení, k jakým citlivým údajům se přistupuje průzkumem rolí a oprávnění v Oracle Database.</li><li>• Použití <b>Oracle Security Assessment Tool</b> pro vyhodnocení konfigurace databáze z pohledu zabezpečení, nastavení bezpečnostních politik, stavu uživatelů, rolí a oprávnění.</li></ul>
Citace 84	... v případech, kdy je pravděpodobné, že operace zpracování budou představovat vysoké riziko pro práva a svobody fyzických osob, by měl být <b>správce odpovědný za provedení posouzení vlivu</b> na ochranu osobních údajů, aby vyhodnotil zejména původ, povahu, zvláštnost a závažnost tohoto rizika...	
Citace 91	... <b>Posouzení vlivu na ochranu osobních údajů</b> 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%3A32016R0679>

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: ... <b>...pseudonymizace a šifrování osobních údajů; ...</b>	<ul style="list-style-type: none"><li>• Použití <b>Oracle Advanced Security - Transparent Data Encryption</b> pro šifrování dat.</li><li>• Použití <b>Oracle Advanced Security - Data Redaction</b> pro pseudonymizaci dat u produkčních aplikacích.</li><li>• Použití <b>Oracle Data Masking and Subsetting</b> pro anonymizaci dat u ne-produkčních aplikací.</li></ul>
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 <b>šifrování</b> ...	
Citace 28	Použití <b>pseudonymizace</b> 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%3A32016R0679>

Odkaz	GDPR znění	Řízení bezpečnosti z pohledu Oracle Database
Citace 26	Zásady ochrany osobních údajů by se proto neměly vztahovat na <b>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....</b>	<ul style="list-style-type: none"><li>Použití <b>Oracle Data Masking and Subsetting</b> pro maskování či anonymizaci dat v ne-produkčním prostředí.</li></ul>
Článek 5	Osobní údaje musí být: přiměřené, relevantní a omezené na nezbytný rozsah ve vztahu k účelu, pro který jsou zpracovávány („ <b>minimalizace údajů</b> “);	<ul style="list-style-type: none"><li>Použití <b>Oracle Data Masking and Subsetting</b> pro vytvoření podmnožiny dat, odstraněním či vytažením části dat na jiné umístění.</li></ul>
Článek 20	Subjekt údajů má právo získat osobní údaje, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, <b>a právo předat tyto údaje jinému správci ...</b>	

# Ochrana proti **útokům** (pokračování)

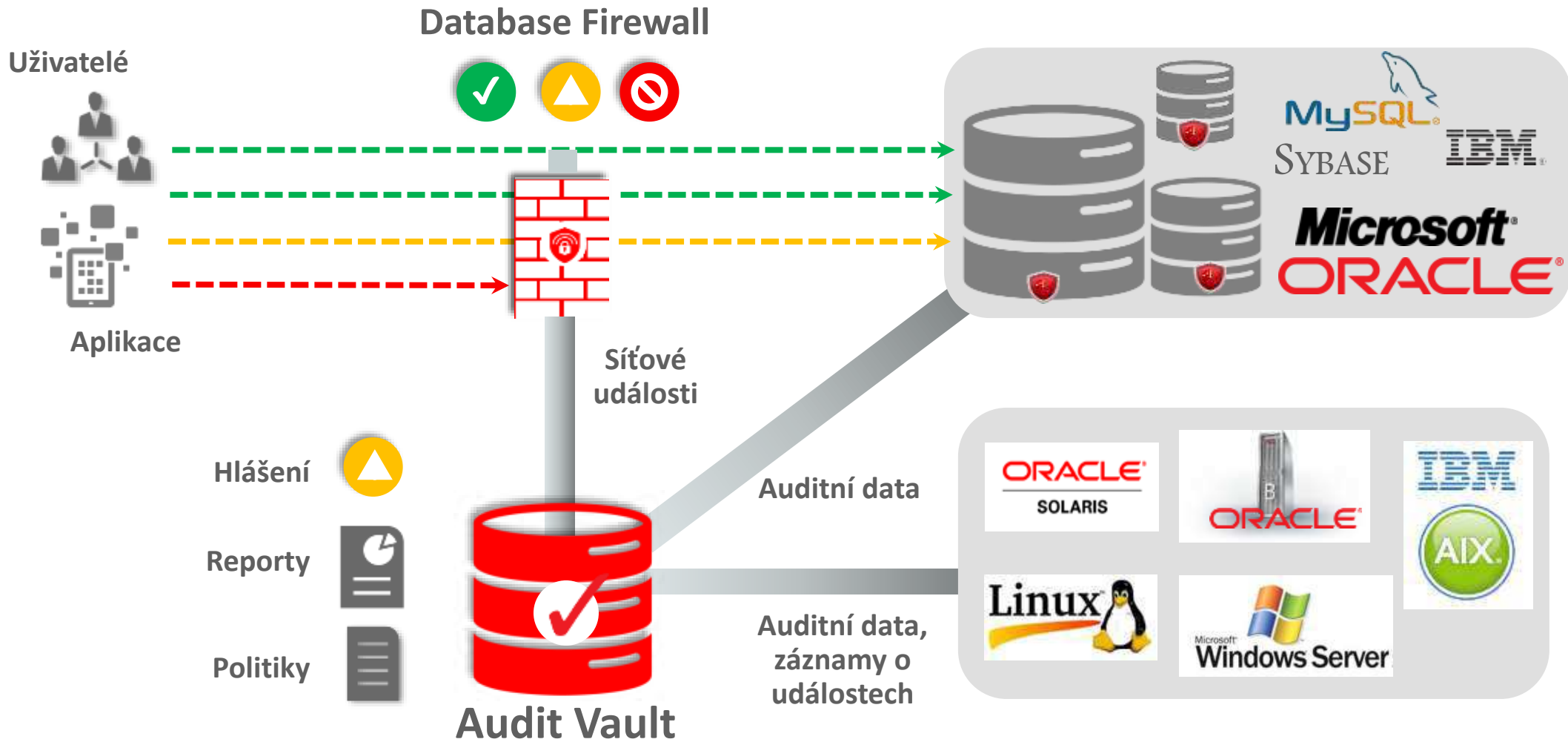
<http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0679>

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 ...	<ul style="list-style-type: none"><li>• Použití <b>Oracle Virtual Private Database</b> pro detailní řízení přístupu k údajům</li><li>• Použití <b>Oracle Label Security</b> pro klasifikaci a označení údajů podle citlivosti obsažené informace</li></ul>
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 ...	<ul style="list-style-type: none"><li>• Použití <b>Oracle Label Security</b> pro řízení přístupu na základě klasifikace údajů</li><li>• Použití <b>Oracle Database Vault</b> pro řízení přístupu privilegovaných uživatelů, kteří zpracovávají data.</li></ul>
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...	<ul style="list-style-type: none"><li>• Použití metod <b>Oracle Strong Authentication</b> jako např. SSL nebo Kerberos spolu s <b>Real Application Security (RAS)</b> pro ověření identity databáze a aplikačních uživatelů přistupujících k citlivým údajům.</li></ul>

# Monitorování za účelem **odhalení hrozby**

<http://eur-lex.europa.eu/legal-content/CS/TXT/?uri=CELEX%3A32016R0679>

Odkaz	GDPR znění	Řízení bezpečnosti z pohledu Oracle Database
Článek 30	Každý správce a jeho případný zástupce vede <b>záznamy o činnostech zpracování</b> , za něž odpovídá. ...	<ul style="list-style-type: none"><li>• Použití <b>Oracle Database Auditing</b> pro sledování a údržbu záznamů (auditních záznamů) během práce s daty.</li><li>• Použití <b>Oracle Fine Grained Auditing</b> pro záznam či audit specifických aktivit uživatelů jako např. výběr citlivých dat apod.</li><li>• Použití <b>Oracle Audit Vault and Database Firewall</b> pro centrální řízení záznamů o aktivitách a zpracování dat.</li><li>• Použití <b>Oracle Audit Vault and Database Firewall</b> pro monitorování a zasílání upozornění na podezřelé chování.</li></ul>
Citace 82	Aby správce nebo zpracovatel doložil soulad s tímto nařízením, měl by vést <b>záznamy o činnostech zpracování</b> , za které odpovídá. ...	
Článek 33	Jakékoli <b>porušení zabezpečení osobních údajů</b> správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, <b>ohlásí</b> 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%3A32016R0679>

Odkaz	GDPR znění	Oracle Database Security Control
Článek 25	...zavede správce <b>jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření</b> , 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.	<ul style="list-style-type: none"><li>Použití <b>Oracle Database Security maximum security architecture</b> pro ochranu dat, jak uvnitř databáze, tak příchodích dat, dále pak návrh nasazení řídicích prvků do architektury, sloužících pro posouzení citlivých dat, návrh preventivních ochranných a v neposlední řadě návrh detektivních činností, když je nutné identifikovat původce zneužití údajů.</li></ul>
Článek 32	Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména <b>náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.</b>	

# Řízení bezpečnosti z pohledu Oracle

ADMINISTRACE	PREVENENCE	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®

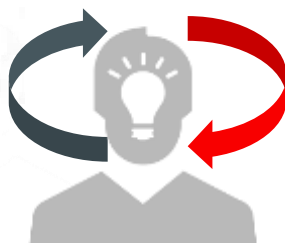


ORACLE®



# Stabilní strategie pro bezpečnost Oracle Database

## PŘEDVÍDÁNÍ HROZEB A JEJICH ZMÍRNĚNÍ



**Transparent** Data Encryption, DBA Control, Redaction, Masking, Privilege Analysis, DB Firewall, RAS, Cloud, ...

## DEFENSE-IN-DEPTH SECURITY CONTROLS



**Překrývající se prvky:** Šifrování, maskování, audit, monitorování, řízení přístupu, redakce, ...

## SECURITY INSIDE-OUT



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

## ZKUŠENOST S NASAZENÍM



**Napříč různými systémy:** Operační systémy, heterogenní databáze, aplikace, ...



[/OracleDatabase](#)



[/OracleSecurity](#)



[blogs.oracle.com/  
SecurityInsideOut](https://blogs.oracle.com/SecurityInsideOut)

[blogs.oracle.com/  
datamasking](https://blogs.oracle.com/datamasking)



[Oracle Database Insider](#)



[/Oracle/database](#)

[/OracleLearning](#)

[oracle.com/database/security](https://oracle.com/database/security)  
[oracle.com/technetwork/database/security](https://oracle.com/technetwork/database/security)

# Integrated Cloud

## Applications & Platform Services

ORACLE®