



Ochranné mechanizmy a procedúry pre bezpečnú prevádzku cloudu

Viktor Němec

27.5.2021

Safe harbor statement



The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

Zákazníci se ptají...

A některé odpovědi jsou jednodušší, než byste možná čekali

Jsou má data
uložená v cloudu
opravdu bezpečná?

Jaké jsou technické
prostředky pro zajištění
bezpečnosti mých dat?

GDPR? US Cloud law?



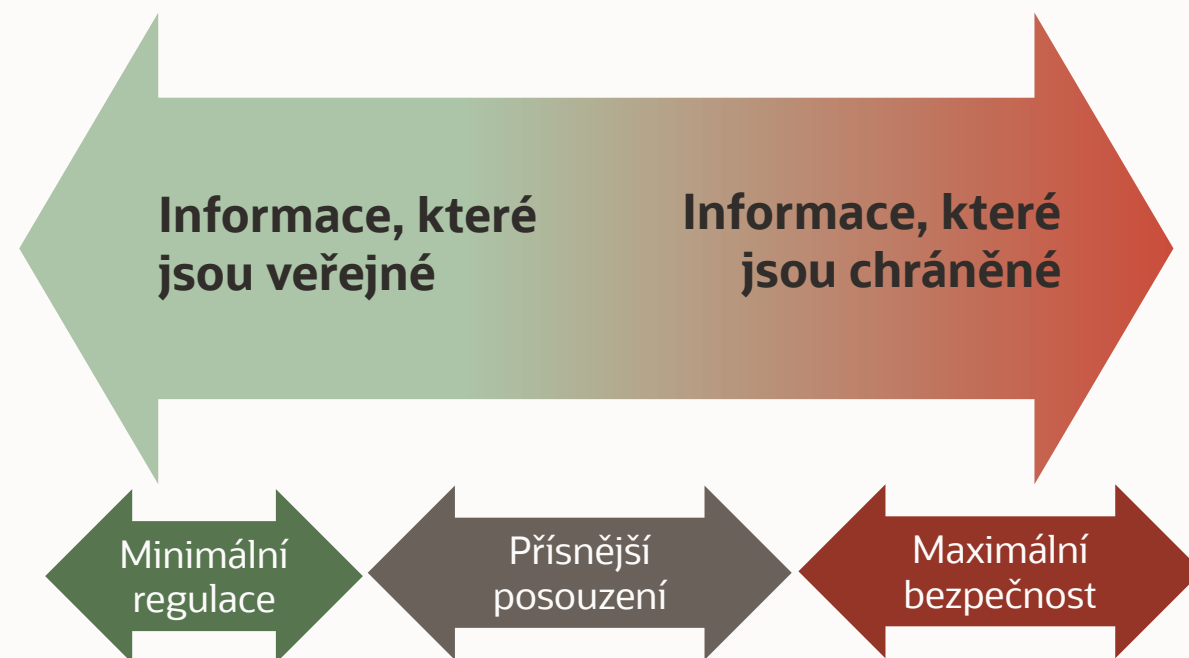
Mohu se o bezpečnostních
pravidlech nějak přesvědčit?

Kde jsou moje data? Mohu
se na ně jít podívat?

Jak se řeší incidenty?

Bezpečnost by měla být přiměřená

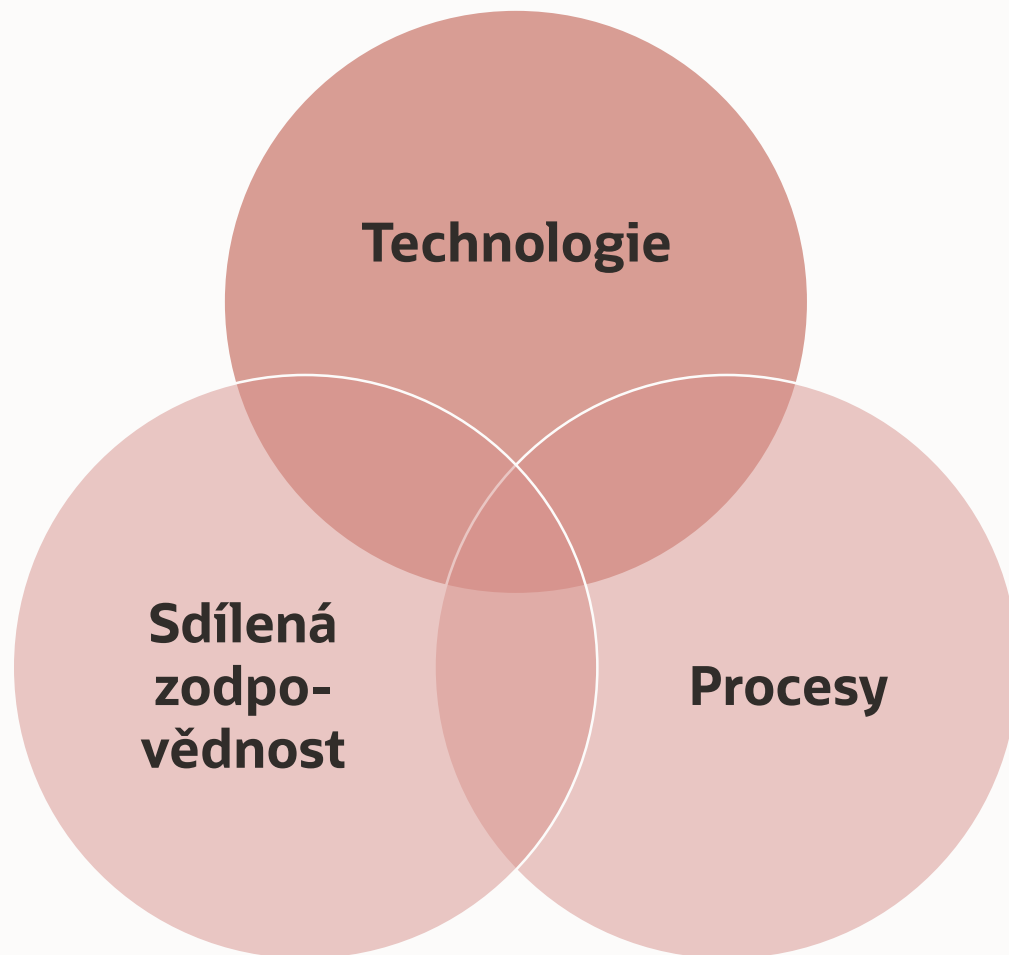
Vyvažujeme tři aspekty



Při využívání cloud computingu poskytovatelem finančních služeb... se **uplatňuje zásada přiměřenosti**. Podle zásady přiměřenosti není poskytovatel finančních služeb oprávněn zcela vyloučit uplatnění kteréhokoli z pravidel obsažených v právních předpisech, ale způsob jejich uplatnění by měl odpovídat povaze, rozsahu a komplexnosti dotčených činností, souvisejícím rizikům a dalším relevantním okolnostem případu.

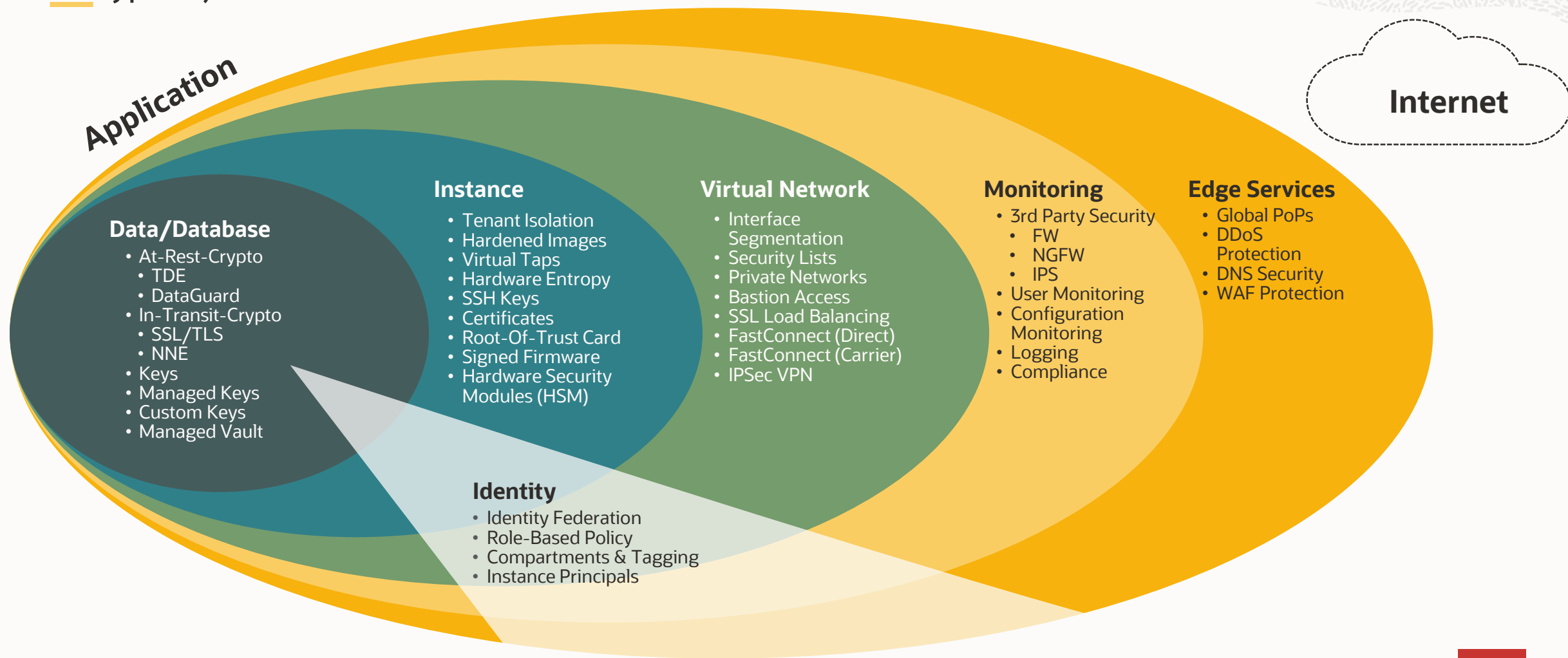
Věstník ČNB ze dne 19.8.2016 k výkonu činnosti na finančním trhu – Cloud Computing

Základní oblasti pro odpovědi na otázky ohledně bezpečnosti jsou tři



První odpověď: Bezpečnostní prvky na všech úrovních

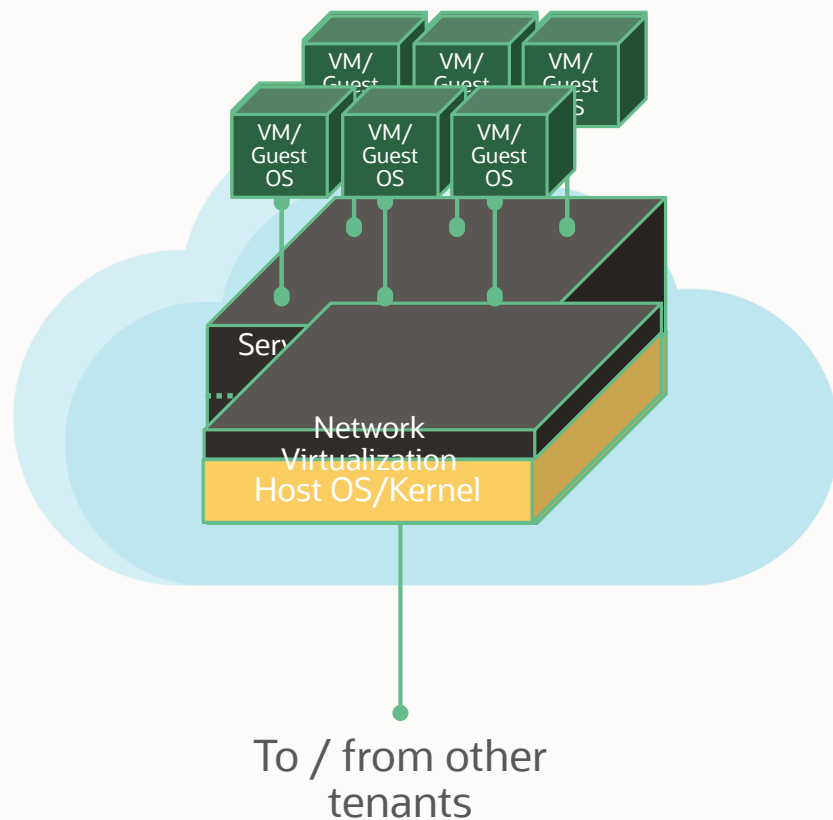
Takto komplexně zabezpečená architektura na všech vrstvách se vyplatí jen v cloudu



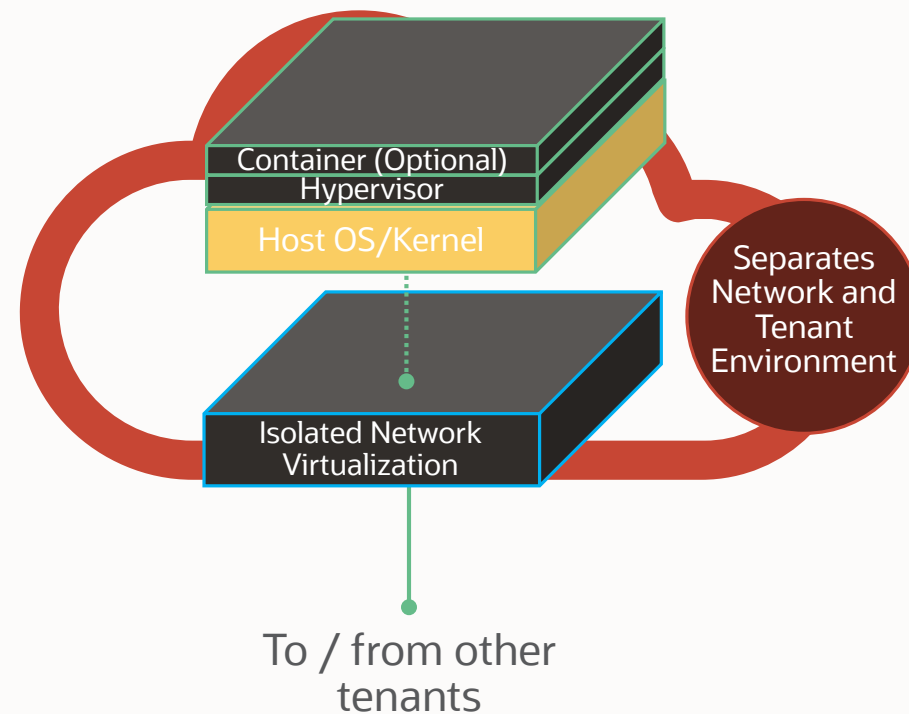
Jeden zajímavý technický detail OCI

Úplné oddělení síťové virtualizace

1st Generation Clouds:
Most prevalent today



2nd Generation Cloud:
Oracle Cloud Infrastructure wide

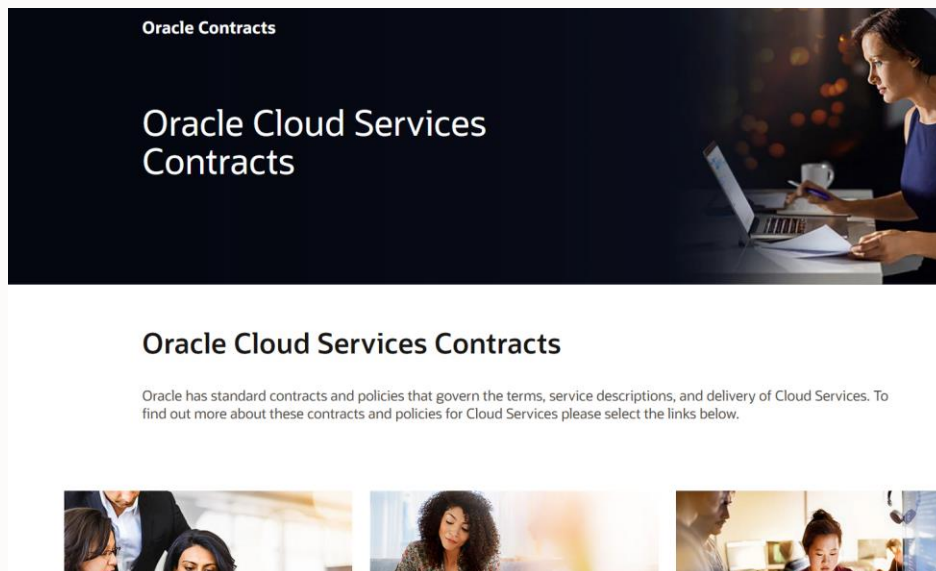


Druhá odpověď: Informace o principech, procesech a dalších detailech dodávky cloudových služeb jsou veřejné

<https://www.oracle.com/corporate/contracts/cloud-services/>

Základní kontrakty jsou tři

- **Cloud Services Agreement** – smluvní vztah se zákazníkem (lze upravit)
- **Data Processing Agreement** – principy zpracování dat, která jsou uložena v našem cloudu
- **Hosting Delivery Policies** – technické detaily dodávky cloudových služeb



Cloud kontrakt se řídí právem České/Slovenské republiky a Zákazník i Oracle souhlasí s výlučnou pravomocí a příslušností soudů v České/Slovenské republice pro řešení jakéhokoli sporu vzniklého z této Smlouvy nebo v souvislosti s ní.

Oracle a certifikace

Procesy jsou důkladně auditovány a potvrzeny mezinárodní certifikací



System and Organization Controls (SOC) 1

System and Organization Controls (SOC) 2



International Organization for Standardization (ISO)/IEC 20000-1:2018

International Organization for Standardization (ISO)/IEC 9001:2015

International Organization for Standardization (ISO)/IEC 27001:2013

International Organization for Standardization (ISO)/IEC 27017:2015

International Organization for Standardization (ISO)/IEC 27018:2014



GDPR – EU

Binding Corporate Rules for Data Processors



VLÁDNY CLOUD

Registrace služeb pro
slovenský vládní cloud

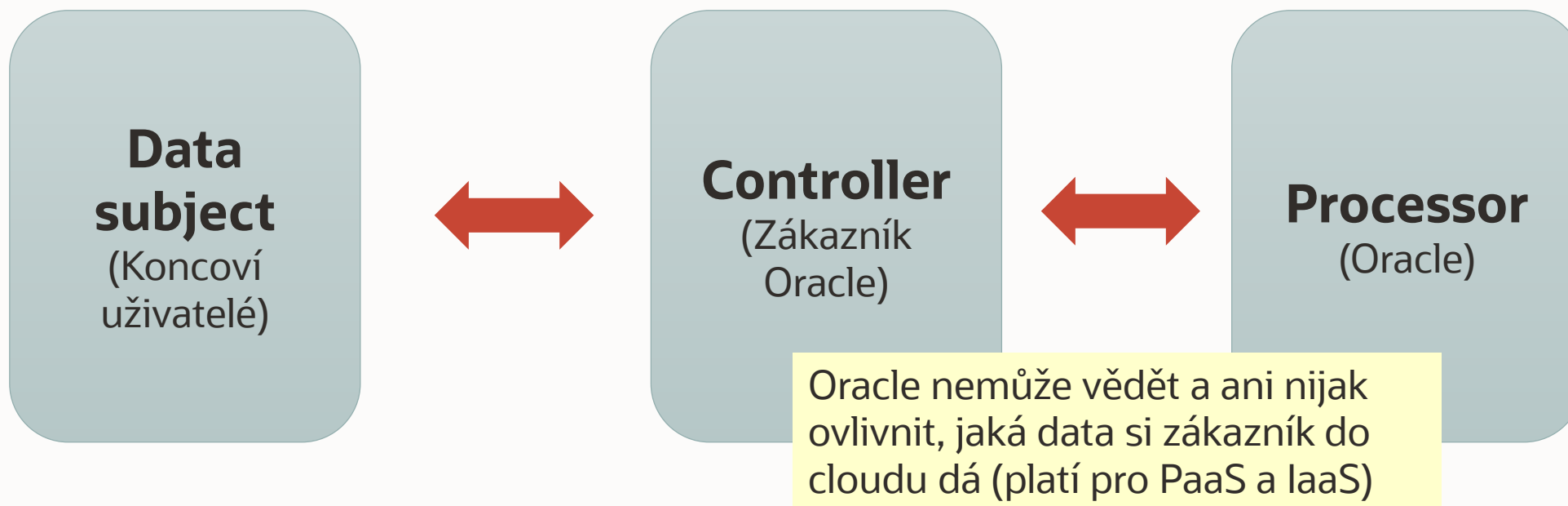
<https://www.oracle.com/cloud/cloud-infrastructure-compliance/>



Oracle a GDPR

Oracle je ve vztahu k GDPR v roli „Processor“

- Oracle získal schválení svých interních provozních předpisů evropskou komisí („Binding Corporate Rules for Data Processor“)
- Ochrana dat je sdílená zodpovědnost a Oracle se zavazuje splnit svoji roli „Processora“



Třetí odpověď: Bezpečnost je sdílená zodpovědnost



Zodpovědnost zákazníka za podpory Oracle



Zodpovědnost Oracle

Application Compliance	PCI, SOX, GDPR
Application Data Security	Customer-managed encryption
Identity Access Security	Use IAM policies
VCN Security	Use VCN security lists/sub-nets/bastions, VPN etc.
DBaaS Security	TDE enabled instances, Oracle DB security best practices etc.
Storage Security	Use bucket ACLs, review access logs etc.
Compute Security	Use instance firewalls, protect SSH keys, security patching etc.
Infrastructure Compliance	SOC 1/2, ISO 27001 etc.
Data Security	Customer data encryption, key management etc.
Operator Access Security	Smart-cards, audit logs etc.
Console and API Security	TLS1.2 ciphers, brute-forcing mitigations etc.
Control Plane Host Security	Access controls, patching, monitoring etc.
Server Hardware Security	Firmware, processors, GPUs, peripherals etc.)
Network Security	DDoS protection, border/transit firewalls, Routers, VPN etc.
Data Center Security	Physical security, personnel vetting, drive destruction etc.

Jak je to s „data residency“?

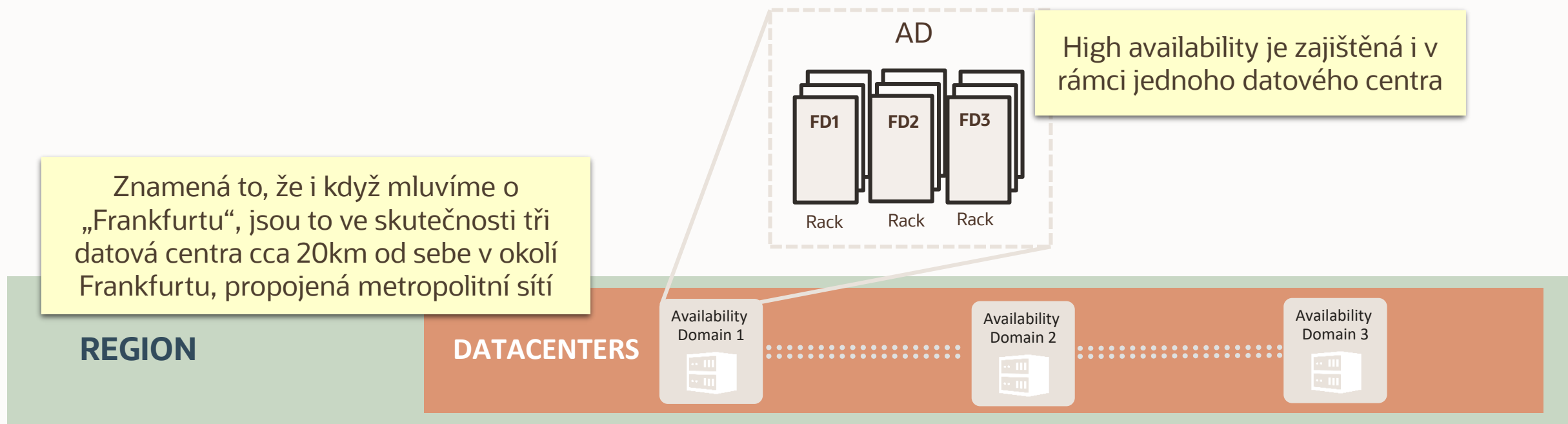
Zákazník si vždy vybírá, ve kterém přesně datovém centru jeho služby poběží



Jak je zajištěna dostupnost?

HA architektura v rámci jednoho regionu

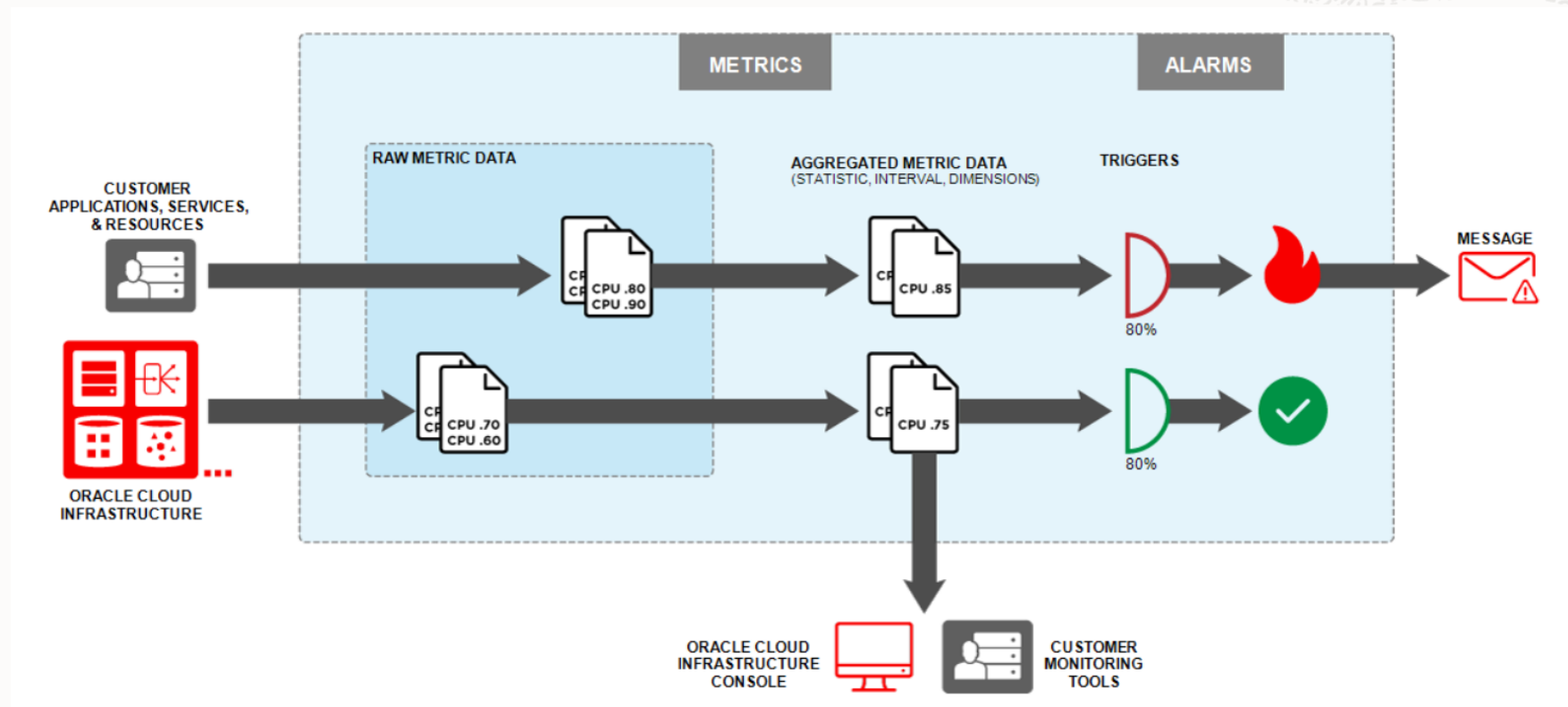
- Multiple fault de-correlated, completely independent datacenters: Availability Domain (AD)
- Grouping of hardware and infrastructure within an AD: Fault Domain
- Predictable low latency & high speed, encrypted interconnect between ADs



Monitorování infrastruktury

Lze přes API integrovat i do jiných monitorovacích nástrojů

Poskytujeme širokou škálu možností, jak monitorovat infrastrukturu:



- Penetrační testy
 - Oracle dělá pravidelné penetrační testy
 - Umožňujeme zákazníkům udělat si zátěžový i penetrační test (po domluvě)

Nabízí Oracle SLA?

A co se stane, když jej nedodržíme?

Příklad služby

SKU	CLOUD SERVICE
B88313	Oracle Cloud Infrastructure - Compute - Bare Metal Dense I/O - X5 - OCPU Per Hour
B88314	Oracle Cloud Infrastructure - Compute - Bare Metal High I/O - X5 - OCPU Per Hour
B88315	Oracle Cloud Infrastructure - Compute - Bare Metal Standard - X5 - OCPU Per Hour
B88316	Oracle Cloud Infrastructure - Compute - Virtual Machine Dense I/O - X5 - OCPU Per Hour
B88317	Oracle Cloud Infrastructure - Compute - Virtual Machine Standard - X5 - OCPU Per Hour

Příklad SLA

Monthly Uptime Percentage for Regions with several Availability Domains

Less than 99.99% but equal to or greater than 99.0%
Less than 99.0% but equal to or greater than 95.0%
Less than 95.0%

Service Credit Percentage

10%
25%
100%

<https://www.oracle.com/assets/paas-iaas-pub-cld-srvs-pillar-4021422.pdf>

Co se stane, když si státní orgán vyžádá osobní data?

Může se jednat o lokální nebo mezinárodní požadavek

- Oracle opravdu neví, jaká data máte uložena ve vašich databázích, které běží v OCI a ani k nim nemá přístup (viz technická architektura)
- Jediné co může Oracle udělat je, předat příslušnému orgánu zašifrovaný datový soubor. Klíče k rozšifrování nemáme. Pokud víte, jak funguje TDE, tak je jasné, že ten soubor nikomu a k ničemu nebude.
- Pokud je aplikován princip přiměřenosti (viz předch. slajd), tak asi není problém stejně data vydat

Ale stejně:

1. Proběhne interní posouzení, jestli je požadavek validní a právně závazný
2. Pokud je požadavek shledán jako nevalidní, podáváme odpor podle příslušných zákonů
3. Automaticky informujeme zákazníka a žádáme o odklad dokud se zákazník nebude moct k požadavku vyjádřit a přijmout potřebné kroky na své straně
4. Pokud požadavek státního orgánu spadá pod utajení, podáváme žádost aby byl odtajněn
5. Veškeré kroky, popsané v předchozích bodech dokumentujeme
6. Minimálně jednou za rok podáváme zákazníkovi podrobnou zprávu o těchto událostech (pokud nastaly)

Odkaz: <https://www.oracle.com/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf>

Má zákazník právo na audit?

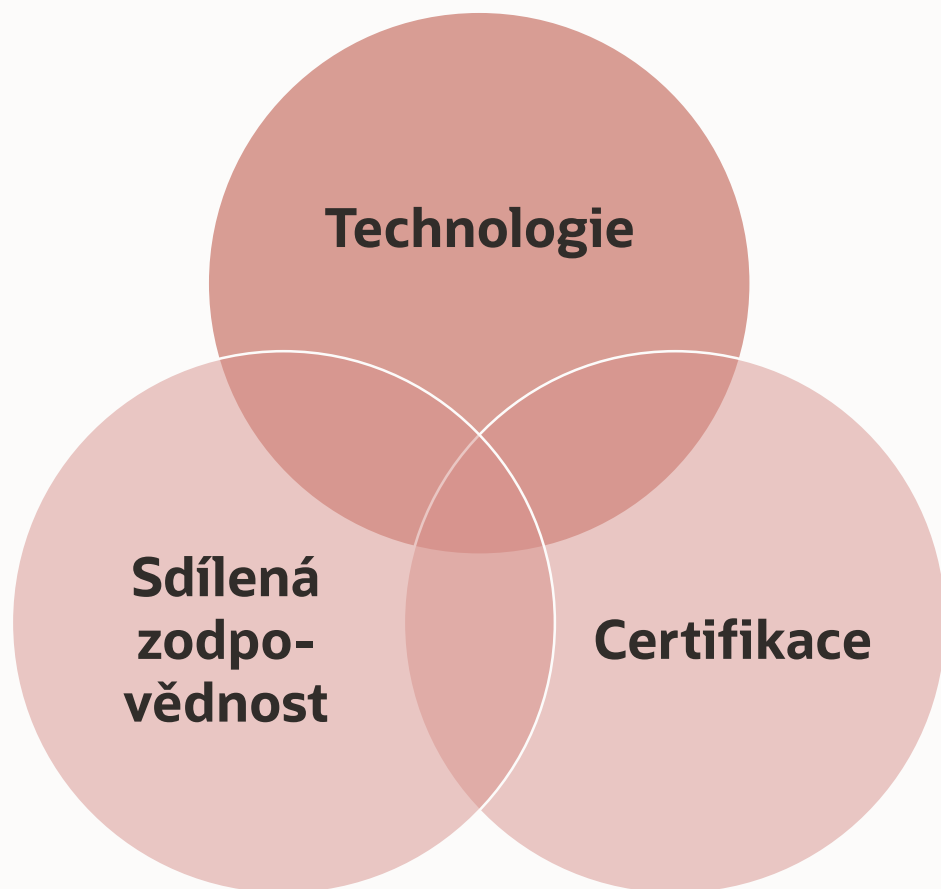
Samozřejmě že ano, přičemž platí tato procedura

1. Zákazník zašle požadavek k auditu a specifikuje oblasti, které chce auditovat
2. Oracle poskytne auditní zprávu od nezávislého auditora, která pokrývá příslušné oblasti
3. Oracle umožní zákazníkovi přímou komunikaci s nezávislým auditorem
4. Pokud body 2. a 3. nestačí tak umožníme zákazníkovi provést vlastní audit za těchto podmínek:
 - Proběhne na náklady zákazníka
 - Maximálně jednou za rok (pokud zákon nestanoví jinak)
 - Auditor je přijatelný pro Oracle a podepíše s Oracle NDA
 - Auditor seznámí Oracle se svojí zprávou a umožní společnosti Oracle se k ní vyjádřit

Odkaz: <https://www.oracle.com/a/ocom/docs/corporate/bcr-privacy-code-051719.pdf>

Shrnutí

Tři hlavní elementy bezpečnosti dat v cloudu



Je potřeba vyvážit





ORACLE