Microsoft

GDPR a dodavatelé IT

Jiří Černý, Ředitel pro právní záležitosti ČR/SK
Microsoft s.r.o.

This presentation is intended to provide an overview of GDPR and is not a definitive statement of the law.

Vymezení role dodavatele IT - poskytovatele Cloudu

- **Správce:** osoba, nebo orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů

(zákazník poskytovatele cloudové služby)

- **Zpracovatel:** osoba, orgán veřejné moci, agentura nebo **jiný subjekt, který zpracovává osobní údaje pro správce**

(poskytovatel cloudové služby)

- **Subjekt osobních údajů:** fyzická osoba, která je identifikovaná , resp. identifikovatelná s použitím osobních údajů

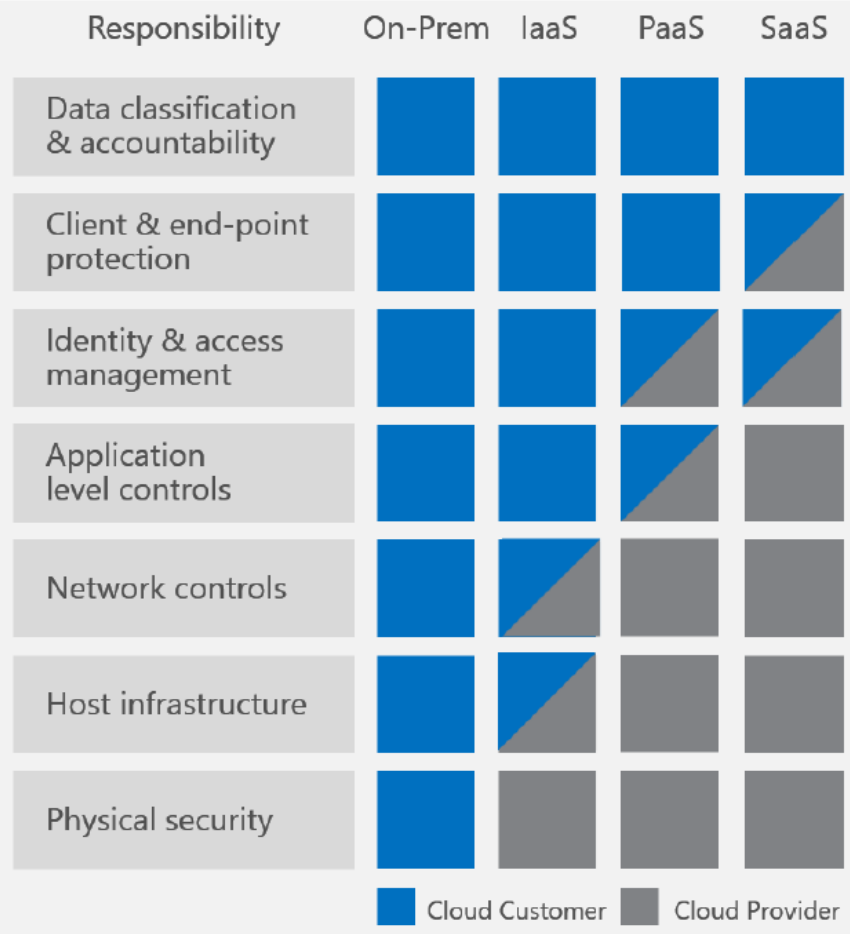
(zákazník, zaměstnanec správce, pacient poskytovatele zdravotnické péče)

- **GDPR mimo Cloud** – MS nemá roli zpracovatele

Sdílená zodpovědnost za bezpečnost v cloudu

Shared responsibilities

Microsoft understands how different cloud service models affect the ways that responsibilities are shared between CSPs and customers.



Q: Jak se staví Microsoft k použití SW při zpracování on-premise

A: MS nemá roli zpracovatele

Viz Product Terms quotation:

19. Zpracování osobních údajů

V rámci svojí role zpracovatele a dílčího zpracovatele osobních údajů v souvislosti s produktem nebo poskytováním odborných služeb společnost Microsoft přijímá závazky v souladu s obecnými podmínkami nařízení Evropské unie o ochraně osobních údajů v příloze 4 podmínek služeb online vůči všem zákazníkům s účinností ke dni 25. května 2018.

Viz Trust Center – whitepaper Shared Responsibilities for Cloud Computing

Jak může zpracování v cloudu pomoci?

- Některé funkce spojené s **výkonem práv subjektů** dat (čl. 12 až 20)
  - Nalezení osobních údajů, přístup, omezení, protokolární výmaz, přenositelnost
- Reflektovat **smluvní požadavky na zpracovatele** (čl. 28)
- Pořizování **záznamů o činnostech zpracování** (čl. 30 bod 2.)
- Implementace **pseudonymizace a šifrování** dat (čl. 25, 32)
- Pomoc při šetření a ohlašování **bezpečnostních incidentů** (čl. 33, 34)
- **Modelové posouzení vlivu** na ochranu os. údajů – DPIA (čl. 35)
- **Zavedení** technických a organizačních **opatření** (čl. 32)

Kde najdeme Technická a organizační opatření

OST – Podmínky pro služby Online – seznam bezp. opatření:

- OST str. 12 – 14: seznam bezp. opatření ve struktuře ISO 27001:2013
- OST str. 14: závazek pokračovat s průmyslovými certifikacemi

Trust Center:

www.microsoft.com/trust

Podklady - členění podle:

- Rolí – Risk / Compliance / Security / BDM
- Principů – Security / Transparency / Privacy…
- Cloud. služeb – Azure, O365, D365…
- Odtud „More reports….“:

Service Trust Platform

https://servicetrust.microsoft.com/ (vyžaduje user credentials)

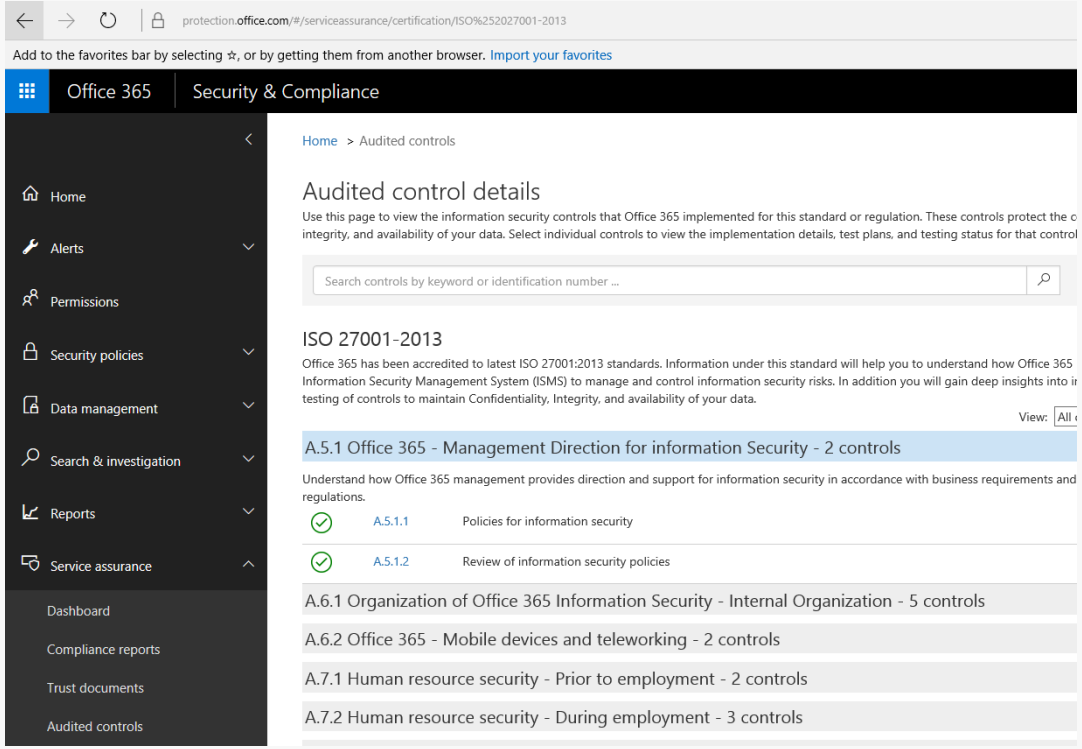
také aka.ms/STP

Repository podkladů k certifikacím:

- Compliance Reports (ISO 27k a SOC reports)
- Trust documents (security whitepapers)

O365 Service Assurance

https://protection.office.com



Jak uchopit GDPR

1. **Mapujte** — Zjistěte, jaké osobní údaje máte a kde se nacházejí
2. **Spravujte** — Rozhodujte o způsobech využití a udělení přístupu k osobním údajům
3. **Chraňte** — Zaveďte bezpečnostní opatření k předcházení, detekování a zvládání bezpečnostních incidentů
4. **Dokumentujte** — Uchovávejte požadovanou dokumentaci, vč. žádostí týkajících se správy osobních údajů či případů porušení zabezpečení

1 Mapujte:

Zjistěte, jaké osobní údaje máte, kde se nacházejí, kdo/co k nim má přístup

Co všechno hledat:

Jakékoli atributy, které mohou vést k identifikaci subjektu údajů

- Jméno
- Emailová adresa
- Příspěvky na sociálních sítích
- Fyzické, fyziologické nebo genetické informace
- Info o zdravotním stavu
- Lokalizační údaje
- Bankovní údaje
- IP adresa
- Cookies
- Kulturní atributy

Inventarizace:

Identifikujte místa uchování osobních údajů, možné přístupy k nim, mapy toků dat

- Emaily
- Dokumenty
- Databáze
- Přenosná média
- Metadata
- Logy - záznamy
- Backupy

Příklady řešení

Microsoft Azure
Microsoft Azure Data Catalog

Enterprise Mobility + Security (EMS)
Microsoft Cloud App Security

Dynamics 365
Audit Data & User Activity
Reporting & Analytics

Office & Office 365
Data Loss Prevention
Advanced Data Governance
Office 365 eDiscovery

SQL Server and Azure SQL Database
SQL Query Language

Windows & Windows Server
Windows Search, Windows PowerShell

2 Spravujte:

Účely a scénáře využití údajů, správa souhlasů, pravidla přístupu k údajům

Správa dat:

Vymezení zásad, rolí a odpovědnosti při zpracování a užití osobních údajů

- Souhlas / právní titul
- Životní cyklus:
- V úložišti
- Při zpracování
- Backup
- Archivace
- Recovery
- Doba expirace
- Likvidace

Kategorizace dat:

Organizace a štítkování dat pro zajištění správného použití

- Druhy osobních údajů
- Citlivost
- Kontext / užití
- Vlastnictví dat
- Zaměstnanci
- Administrátoři
- Uživatelé

Příklady řešení

Microsoft Azure

Azure Active Directory
Rights Management Services
Azure Role-Based Access Control (RBAC)

Enterprise Mobility + Security (EMS)

Azure Information Protection

Dynamics 365

Security Concepts

Office & Office 365

Advanced Data Governance
Journaling (Exchange Online)

Windows & Windows Server

Microsoft Data Classification Toolkit

3 Chraňte:

Zaveďte bezpečnostní opatření k předcházení, detekování a zvládání bezpečnostních incidentů

Prevence proti hrozbám:

Zabezpečení dat

- Fyzická ochrana datového centra
- Síťová bezpečnost
- Zabezpečení úložiště
- Počítačová bezpečnost
- Správa identit
- Řízení přístupu
- Šifrování
- Zmírňování rizik

Detekce a zvládání bezpečnostních incidentů:

- Monitorování systému (*System monitoring)*
- Identifikace bezpečnostní incidentů
- Zjišťování dopadů
- Plán pro zvládání incidentů
- Zotavení po incidentu *(Disaster recovery)*
- Metodika ohlašování dozor. orgánu
- Metodika oznamování subjektům dat

Příklady řešení

Microsoft Azure
Azure Key Vault, Azure Security Center
Azure Storage Service Encryption

Enterprise Mobility + Security (EMS)
Azure Active Directory Premium
Microsoft Intune

Office & Office 365
Advanced Threat Protection
Threat Intelligence

SQL Server and Azure SQL Database
Transparent data encryption
Always Encrypted

Windows & Windows Server
Windows Defender Advanced Threat Protection
Windows Hello
Device Guard / Credential Guard

4 Dokumentujte:

Uchovávejte požadovanou dokumentaci, vč. žádostí týkajících se správy osobních údajů či případů porušení zabezpečení

Provozní záznamy

Organizace musí zaznamenávat:

- Logy změn údajů
- Účel zpracování údajů
- Zpracování různých kategorií osob. údajů
- Přístupová oprávnění třetích stran k datům
- Organiz. a technická bezpečnostní opatření
- Doby uchovávání vs. prokazatelné smazání osobních údajů

Dokumentace

Zajistit dokumentaci:

- Dokumentaci zpracování osobních údajů, včetně cloud. „zpracovatele“
- Ohlašování a oznamování případů porušení zabezpečení
- Model správy dat
- Vyřizování žádostí subjektů dat
- Revizní zprávy o souladu
- Archivaci logů

Příklady řešení

Microsoft Trust Center
Service Trust Portal

Microsoft Azure
Azure Auditing & Logging
Microsoft Azure Monitor

Enterprise Mobility + Security (EMS)
Azure Information Protection

Dynamics 365
Reporting & Analytics

Office & Office 365
Service Assurance
Office 365 Audit Logs
Customer Lockbox

Windows & Windows Server
Windows Defender Advanced Threat Protection

Beginning your General Data Protection Regulation (GDPR) journey

Whitepaper 31 stran
Metodika 4 kroků + nástroje
i v češtině

www.aka.ms/GDPRwhitepaperCZ

Od analýzy rizik k DPIA

- Čl. 35: nutné „posouzení vlivu“ pro zpracování s „vysokým rizikem“ (DPIA – Data Protection Impact Assesment)
- Jak může pomoci Zpracovatel osobních údajů:
  - 1. **Hodnocení rizik určitého typu zpracování** osobních údajů
    - Metodika dle VoKB, ISO 27005, ISO 29134 - rizika porušení důvěrnosti, integrity, dostupnosti a ztráty os. údajů
    - Dále rizika ztráty kontroly a nesouladu s regulatorními požadavky pro správce
    - Pro ZoKB: rozsah analýzy rizik pokrývá požadavky VoKB č. 316/2014 Sb.
  - 2. **Nastavení adekvátních technických a organiz. opatření**
  - 3. **Charakteristika zbytkových rizik pro Správce**

Modelové analýzy rizik a scénáře pro DPIA

- GDPR prezentace a zdroje v CZ: www.aka.ms/jaknaGDPR
  k dispozici modelové analýzy rizik pro zákazníky (v češtině):
  - Analýza rizik: **Zdravotnická dokumentace v cloudu Azure** (ICZ a.s.)
    - Znalecký posudek ústavu CETAG: adekvátní úroveň zabezpečení dle GDPR
  - Analýza rizik: **Spisová služba Gordic GINIS v cloudu Azure** (RAC s.r.o.)
  - **Formát DPIA** pro **zpracování osobních údajů v Office 365** (ICZ a.s.)
    - Osobní údaje v Exchange Online
    - Citlivé osobní údaje v SharePoint Online
    - Telemedicína / citlivé osobní údaje přes a upload přes Skype for Business
- Soulad s požadavky GDPR ověřen právní kanceláří Pierstone s.r.o.

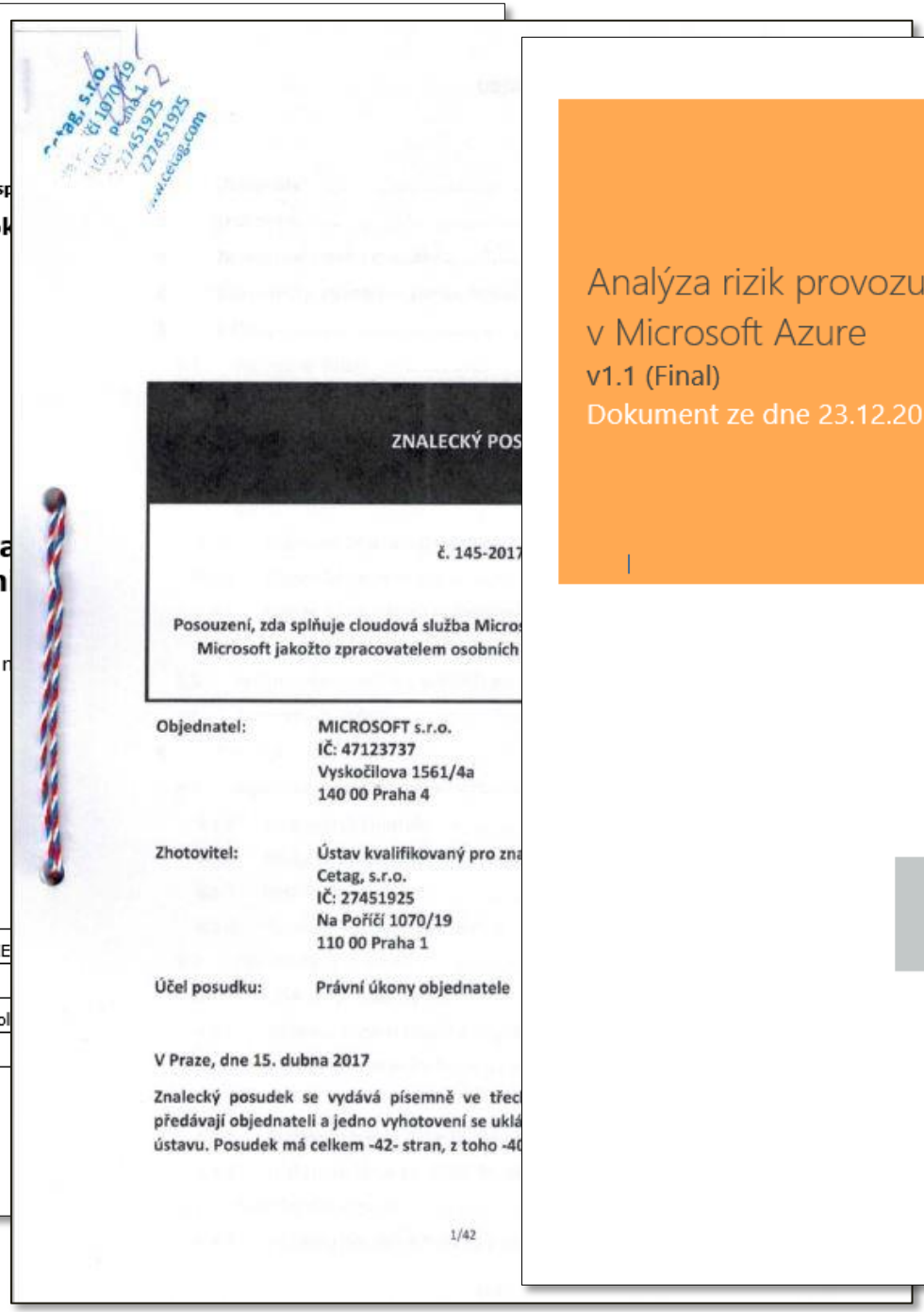
S.ICZ a.s.
Na hřebenech II 1718/10
140 00 Praha 4

Na posouzení právních aspektů sp
PIERSTONE s.r.o., advok
Na Příkopě 9
110 00 Praha 1

Analýza rizik a
zdravotn

Studie zpracovaná n

Dokument:	MICR01451-STUDIE
Zakázka:	MICR.01451
Zpracoval:	Ondřej Steiner a kol
Datum:	16.12.2016


ZNALECKÝ POS

č. 145-2017

Posouzení, zda splňuje cloudová služba Micros
Microsoft jakožto zpracovatelem osobních

Objednatel: MICROSOFT s.r.o.
IČ: 47123737
Vyskočilova 1561/4a
140 00 Praha 4

Zhotovitel: Ústav kvalifikovaný pro zna
Cetag, s.r.o.
IČ: 27451925
Na Poříčí 1070/19
110 00 Praha 1

Účel posudku: Právní úkony objednatele

V Praze, dne 15. dubna 2017

Znalecký posudek se vydává písemně ve třec
předávají objednateli a jedno vyhotovení se uklá
ústavu. Posudek má celkem -42- stran, z toho -4

1/42

Analýza rizik provozu spisové slu
v Microsoft Azure
v1.1 (Final)
Dokument ze dne 23.12.2016

S.ICZ a.s.
Na hřebenech II 1718/10
140 00 Praha 4

Na posouzení právních aspektů spolupracovala
PIERSTONE s.r.o., advokátní kancelář
Na Příkopě 9
110 00 Praha 1

Modelová DPIA a analýza rizik pro zpracování osobních údajů v Microsoft Office 365

Studie zpracovaná na základě poptávky Microsoft s.r.o.

Dokument:	MICR01817-STUDIE-110.docx		
Zakázka:	MICR.01817	**Verze:**	1.1
Zpracoval:	Kolektiv autorů S.ICZ	**Stav:**	finální
Datum:	10.4.2017	**Počet stran:**	137

1/137

Široké portfolio certifikací a mezinárodních standardů

Certifikace a podklady: Microsoft Trust Center www.microsoft.com/trust; Repository: www.aka.ms/STP

GLOBAL

- ISO 27001
- ISO 27018
- ISO 27017
- ISO 22301
- ISO 9001
- SOC 1 Type 2
- SOC 2 Type 2
- SOC 3
- CSA STAR Self-Assessment
- CSA STAR Certification
- CSA STAR Attestation

US GOV

- Moderate JAB P-ATO
- High JAB P-ATO
- DoD DISA SRG Level 2
- DoD DISA SRG Level 4
- DoD DISA SRG Level 5
- SP 800-171
- FIPS 140-2
- Section 508 VPAT
- ITAR
- CJIS
- IRS 1075

INDUSTRY

- PCI DSS Level 1
- CDSA
- MPAA
- FACT UK
- Shared Assessments
- FISC Japan
- HIPAA / HITECH Act
- HITRUST
- GxP 21 CFR Part 11
- MARS-E
- IG Toolkit UK
- FERPA
- GLBA
- FFIEC

REGIONAL

- Argentina PDPA
- EU Model Clauses
- UK G-Cloud
- China DJCP
- China GB 18030
- China TRUCS
- Singapore MTCS
- Australia IRAP/CCSL
- New Zealand GCIO
- Japan My Number Act
- ENISA IAF
- Japan CS Mark Gold
- Spain ENS
- Spain DPA
- India MeitY
- Canada Privacy Laws
- Privacy Shield
- Germany IT Grundschutz workbook

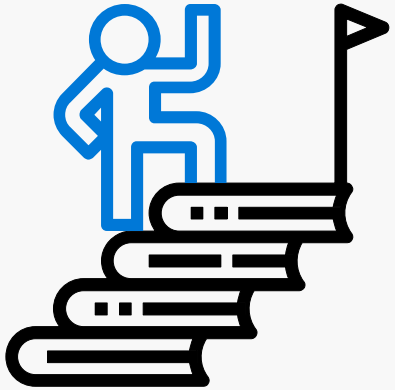
Shrnutí

Zjednodušení cesty k souladu

Využijte ověřená řešení v cloudu s využitím delegace odpovědností na zpracovatele

Posouzení rizik a realizace opatření

Využijte služby a nástroje pro pokrytí rizik a pružné zavedení adekvátních bezpečnostních opatření



Využití expertních znalostí

Unikátní kompetence partnerské sítě spol. Microsoft v oblasti řízení rizik, procesů, a právního poradenství

Zdroje k GDPR:

Microsoft Corp hlavní stránka:
microsoft.com/GDPR

Prezentace a zdroje v češtině:
aka.ms/jaknaGDPR

Microsoft Trust Center
microsoft.com/trust

Service Trust Platform – podklady k certifikacím, auditní zprávy: aka.ms/STP
(vyžaduje log-in, NDA level)

Microsoft

Děkuji Vám za pozornost

Jiří Černý

jiric@microsoft.com