

GDPR Akademie:

Efektivní vyhledávání, řízení a zabezpečení osobních informací
v dokumentech a v e-mailech

Vlastimil Tesař, Martin Hruška, Petr Špetlík

Agenda

- Vymezení základních pojmů, Microsoft a GDPR
- Správa osobních informací v dokumentech a emailech
- Ukázka
- Zabezpečení PC a notebooků
- Zabezpečení mobilních zařízení
- Přehled produktů

Hlavní principy General Data Protection Regulation

- Obecné „nařízení“ o ochraně osobních údajů (přímo aplikovatelné v ČR)
- Transparentnosti při zpracování a používání osobních údajů
- Nově definovaná práva fyzických osob („subjektů údajů“)
- Omezení zpracovávání osobních údajů pouze na stanovené a opodstatněné účely
- Omezení ukládání osobních údajů pouze na dobu nezbytnou pro daný účel
- Zajištění ochrany osobních údajů pomocí náležitých postupů zabezpečení
- Týká se všech organizací v EU nebo pracujících s osobními údaji rezidentů EU
- Účinnost od 25.5.2018
- Sankce až €20m nebo 4% celosvět. obratu společnosti (ve veřejné správě bude „cap“)

Rozšířené povinnosti subjektů údajů – občanů EU

- Právo na informace (o zpracování údajů subjektu)
- Právo na přístup k osobním údajům
- Právo na opravu osobních údajů
- Právo na výmaz
- Právo na omezení zpracování
- Právo na přenositelnost údajů (i přímo správce -> jiný správce)
- Právo vznést námitku
- Právo nebýt předmětem rozhodnutí, založeného výhradně na automatizovaném zpracování, které má pro subjekt údajů právní účinky

Vymezení rolí v GDPR ve vztahu k Microsoftu

- **Správce / Prevádzkovateľ** : osoba, nebo orgán veřejné moci, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů (*firemní zákazník, Vy*)
- **Zpracovatel / Sprostredkovateľ** : osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce
(*v případě cloudové služby Microsoft ve smluvním vztahu se zákazníkem*)
- **Subjekt osobních údajů / Dotknutá osoba** : fyzická osoba, která je identifikovaná , resp. identifikovatelná s použitím osobních údajů (*fyzický zákazník, zaměstnanec, občan*)
- GDPR pro Microsoft mimo Cloud – poskytuje technologie, ale nemá roli Zpracovatele
- Role zpracovatele vůči správci musí být smluvně podložená (viz dále)

Smluvní záruky Microsoft = zpracovatel

Požadavek	Řešení
Smluvní podmínky dle čl. 28	OST - „Podmínky pro služby online“ od září 2017 má standardně přílohu č. 4 – řeší explicitně soulad s články 28, 32 a 33 GDPR. Obsahuje „Podmínky ochrany osobních údajů a zabezpečení“ (str. 8 a dále)
Zabezpečení zpracování – čl. 32	OST kap. „Zabezpečení“ str. 13 a dále - bezp. opatření, certifikace a auditní zprávy Dále Příloha 4 GDPR Odkazy na Trust Center www.microsoft.com/trust Celé auditní zprávy a dokumenty jsou na Service Trust Platform (www.aka.ms/STP)
Místo uložení dat	OST – odst. „Umístění pro uchování neaktivních zákaznických dat“
Místo zpracování dat	Může nastat v jistých případech i mimo EU. Řešení – GDPR čl. 46 Standardní smluvní doložky o ochraně údajů přijaté EC (viz potvrzení EC a vyjádření ÚOOÚ). Zahrnuty jako příloha č. 3 OST. Podrobnosti viz www.microsoft.com/trust , oblast Privacy, „Where your data is located“, „Who can access your data“
Použití a zpřístupnění zákaznických dat	OST – Příloha 4 GDPR, OST – str. 7, Použití zákaznických dat, Zveřejnění (zpřístupnění) zákaznických dat

Sdílená odpovědnost Správce - Zpracovatel



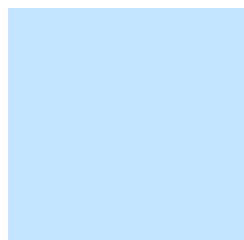
Řízení rizik na straně **Správce**

Kategorizace údajů a stanovení politik ochrany



Sdílené řízení rizik

Správa identit a řízení přístupu k údajům



Řízení rizik na straně **Zpracovatele**

Fyzická bezpečnost a infrastruktura datových center

[Shared responsibility](#) – Microsoft whitepaper

Odpovědnost	On-Prem	IaaS	PaaS	SaaS
Kategorizace údajů a politiky ochrany				
Ochrana koncových zařízení				
Správa identit a řízení přístupu k údajům				
Bezpečnost aplikací				
Síťová infrastruktura v datových centrech				
Virtuální stroje (VM)				
Fyzická bezpečnost				

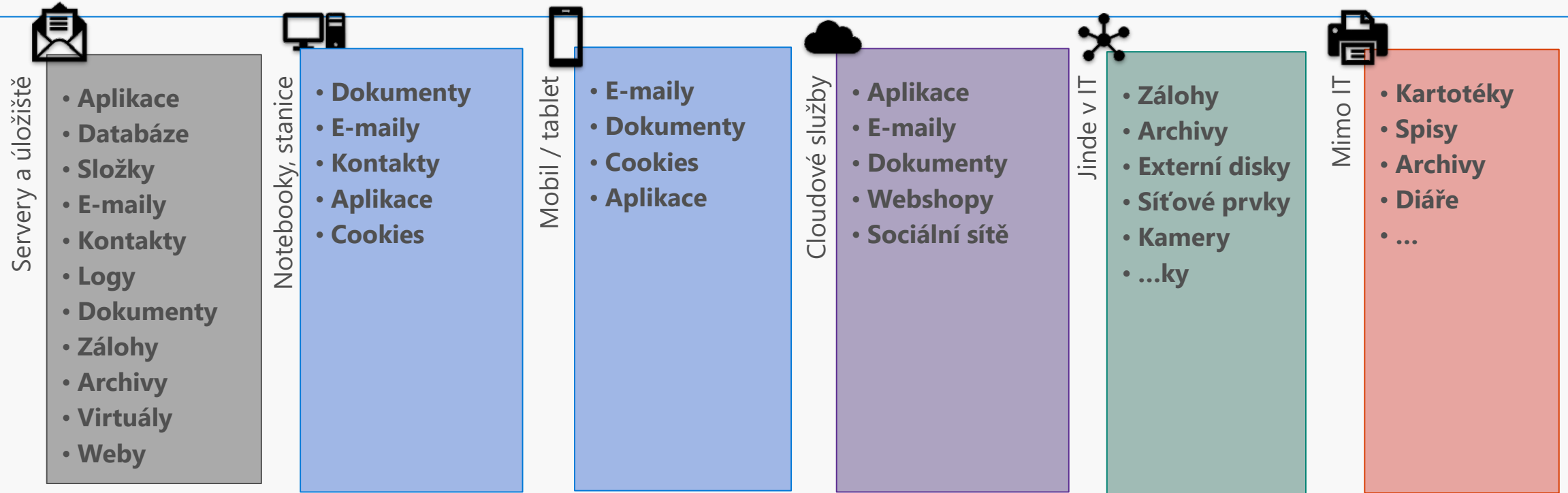


Zákazník cloudu



Provozovatel cloudových služeb

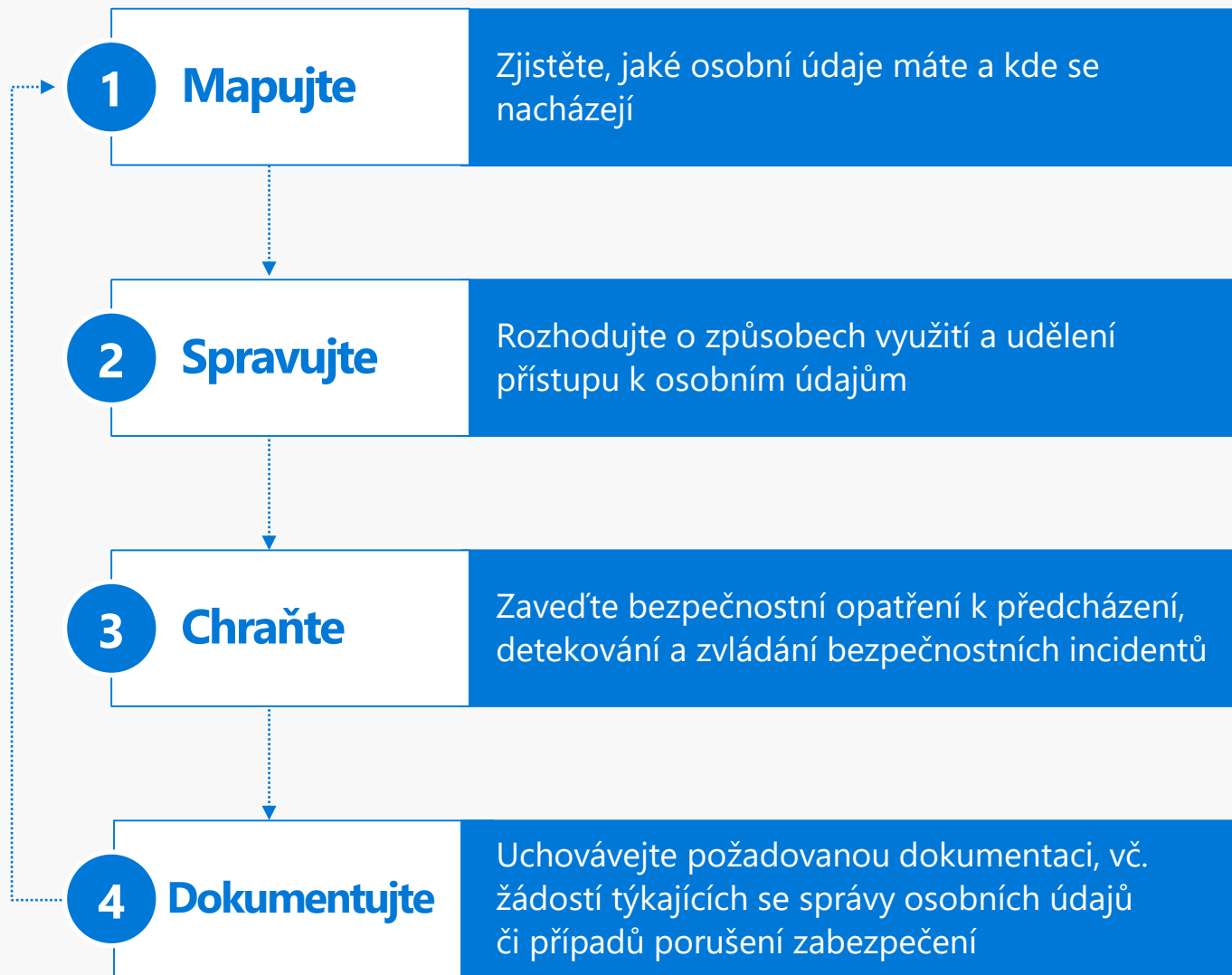
Kde všude leží osobní údaje?



ss



Jak uchopit GDPR



Příprava na obecné nařízení o ochraně osobních údajů (GDPR)

Whitepaper 31 stran
Metodika 4 kroků + nástroje
i v češtině

www.aka.ms/GDPRwhitepaperCZ

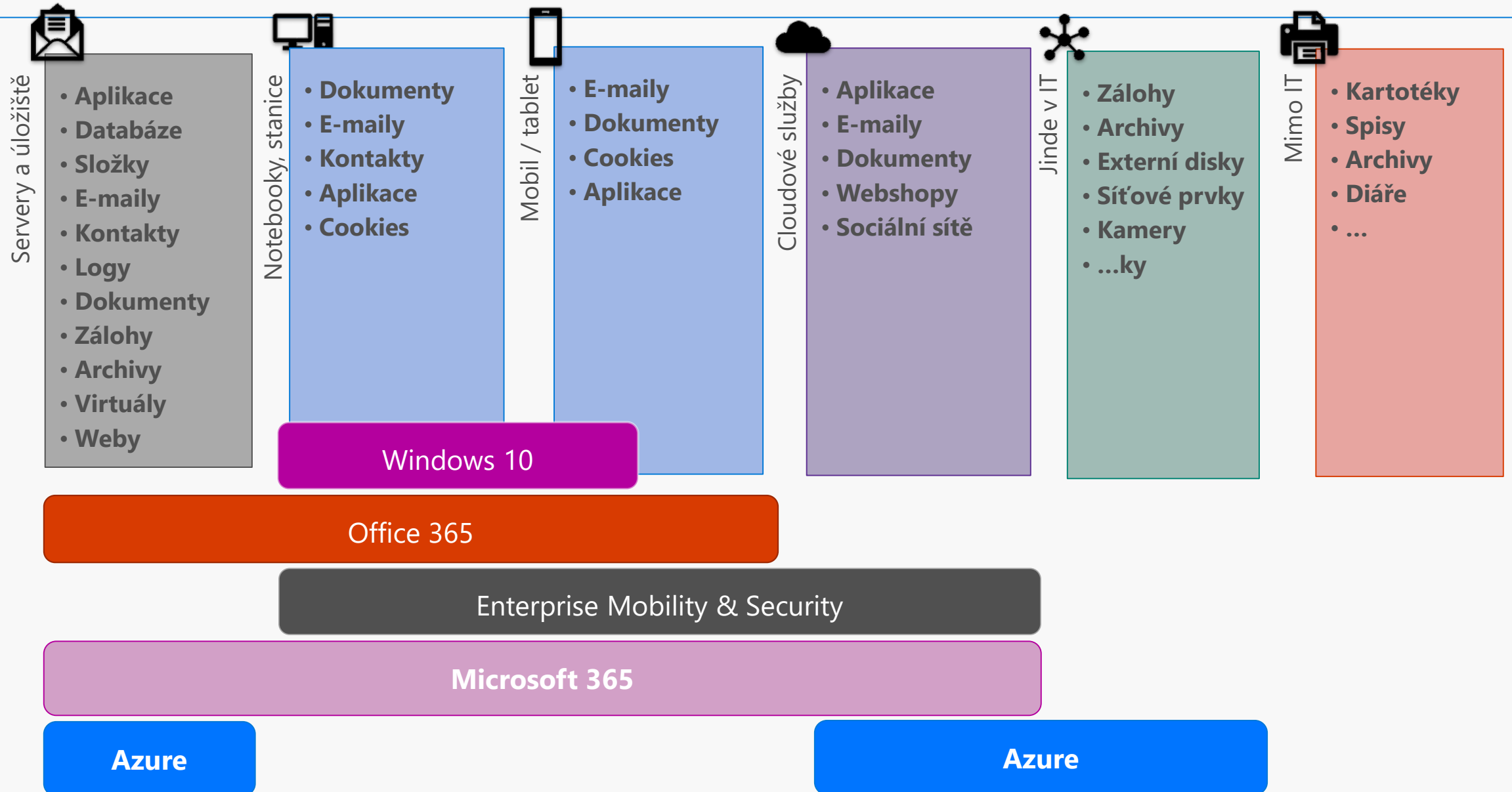
Příprava na obecné nařízení o ochraně osobních údajů (GDPR)

Dosáhněte rychleji souladu s nařízením
GDPR pomocí služby Microsoft Cloud



Jak tedy může Microsoft pomoci

Kde mohou služby Microsoft pomoci?



„Úrovně dopadů“ = vstup pro posouzení rizik

(Uvedené příklady je třeba posuzovat s ohledem na konkrétní obsah a možné dopady)

Zanedbatelný

Telefonní seznam
Seznam účastníků
konference (*pokud něco
neprozrazuje!*)
E-mailové adresy
Patičky e-mailů

*Podráždění jednotlivce,
likvidace nevyžádané
pošty,
potřeba znovu vyplnit
formulář po ztrátě dat*

Omezený

Vyúčtování služebních cest
Fotografie na ID karty
Logy s IP adresami
Zdravotní způsobilost
CV interních zaměstnanců

*Potíže, které však lze
poměrně snadno překonat:
Zvýšené náklady, odmítnutí
některé z komerčních
služeb, obavy,
nedorozumění*

Vysoký

Správní delikty
Daňová přiznání
Informace s výsledkem
psychologického testu
Kárná řízení
CV klientů

*Vážné potíže.
Diskriminace: blacklisting
většinou bank.
Vznik vysokého finančního
závazku.
Ztráta zaměstnání.
Vyloučení v rodině,
v místě bydliště.*

Kritický

Zdravotnická
dokumentace
Registry s citlivými
osobními údaji
Kompromitující materiály
na jednotlivce

*Subjekt se setká s velikými,
až nepřekonatelnými
obtížemi.
Osobní bankrot –
nesplatitelný dluh.
Ohrožení života
(nesprávná medikace).
Dlouhodobé duševní nebo
fyzické onemocnění.*



GDPR a cloud Zabezpečení

Maximální využití technického, bezpečnostního i organizačního zajištění všech cloudových služeb

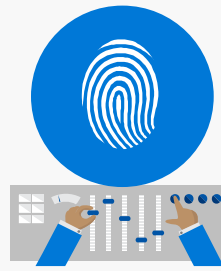
- Ověření uživatelů i správců- Multifaktorová **autentizace**
- **Ochrana** před kybernetickými útoky
- **Šifrování** dat
- **Organizační opatření** v cloudových službách pro přístup k systémům i datům
- Přístup **řízený zákazníkem** – Customer Lock Box
- Zajištěné **logování a audit**y – viz dále

Rozsah služeb viz Smluvní závazky zpracovatele

- Office 365, Microsoft Azure Core, Microsoft Dynamics Core
...

Consumer služby

- Outlook.com, Hotmail, Bing...
- Microsoft není Zpracovatel



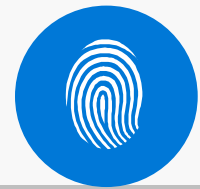
GDPR a cloud

Snížení nákladů

Snížení nákladů, souvisejících s GDPR

- Na **zmapování stávajícího stavu**, kde se nacházejí osobní údaje při analýze (rozdílová analýza, DPIA)
- Na **technická i organizační opatření** pro zajištění provozu a zabezpečení osobních informací a systémů
- Na **vlastní výkon** práv subjektů
- Na případnou **finanční sankci** v případě úniku dat
- Na **ztrátu zákazníků** spojenou se ztrátou důvěry a reputace
- Maximální **využití primárních vlastností Office 365 pro produktivitu uživatelů** a nejen kvůli zabezpečení a GDPR

Zajištění a správa osobních informací
v nestrukturovaných systémech
E-mail & dokumenty



Osobní informace E-maily a dokumenty v Office 365

- **Vyhledání dokumentů a e-mailů**, kontaktů s osobními údaji a informací napříč službami – Vyhledání konkrétních osobních údajů **pověřenými osobami** bez přímých oprávnění k vlastním datům – *eDiscovery a Content Search*
- **Zabezpečení dokumentů a e-mailů** – možnost zneplatnění a omezení přístupu bez ohledu na jejich umístění, omezení odeslání jejich odeslání, nastavení politik a analýza jejich dodržování – *DLP a Information Protection*
- **Minimalizace výskytu** stejných dokumentů s osobními údaji jejich jednoduchým sdílením a ne kopírováním pomocí e-mailových příloh – *propojení s aplikacemi Office*
- Možnosti **vytvoření agend** spojených se zajištěním výkonu práv subjektů – *Activity Hub pro O365, workflow pro Sharepoint Online, Azure*



E-maily a dokumenty mimo Office 365

- **Vyhledání lokálních** dokumentů a e-mailů, kontaktů s osobními údaji a informací napříč lokálními systémy mimo Office 365
 - Lokální počítače – *Windows + Outlook*
 - Windows servery – *Content Search – neumí eDiscovery*
 - *Exchange 2013+, SharePoint 2013+*
- **Zabezpečení lokálních dokumentů a e-mailů** – možnost zneplatnění a omezení přístupu bez ohledu na jejich umístění, omezení jejich odeslání, nastavení politik a analýza jejich dodržování *DLP*
 - *Microsoft EMS nebo Azure Information Protection*
- **Minimalizace výskytu** stejných dokumentů s osobními údaji jejich jednoduchým sdílením a ne kopírováním pomocí e-mailových příloh – *propojení s aplikacemi Office*
- Možnosti **vytvoření agend** spojených se zajištěním výkonu práv subjektů – *Workflow pro Sharepoint*
- Naplánujte si **migraci do Microsoft 365** jako součást opatření – zmapování osobních údajů, nastavení procesů, snížení nákladů na opatření, získání Office a EMS...

Ukázka nastavení ochrany

Information Protection



GDPR



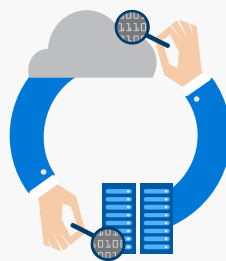
Ochrana PC a notebooků s Windows 10

Zabezpečení zařízení proti napadení a odcizení dat

- **Proaktivní ochrana proti Ransomware** a dalšímu škodlivému kódu *pomocí Device Guard a Applocker*
- **Integrovaný antivirový systém** *Windows Defender Antivirus chrání i proti malware, který ještě nebyl nikde použit*
- **Zabezpečená identita oprávněného uživatele**
Vestavěná podpora vícefaktorového ověření uživatele Windows Hello for Business.

Zabezpečené informací při odcizení nebo ztrátě

- **Firemní a informace osobní data** na zařízeních a uložiscích zabezpečena pomocí technologie Windows Information Protection a Azure Information protection
- **Šifrování obsahu pevného disku** technologií Bitlocker chrání zařízení v případě ztráty nebo odcizení
- **Odolnost proti** útokům zneužívající **zcizení hesla** z paměti zařízení pomocí funkce Credential Guard
- **Zabezpečená identita oprávněného uživatele**



GDPR

Ochrana mobilů a tabletů s EMS

Zajištění zařízení, ze kterého se přistupuje k osobním údajům

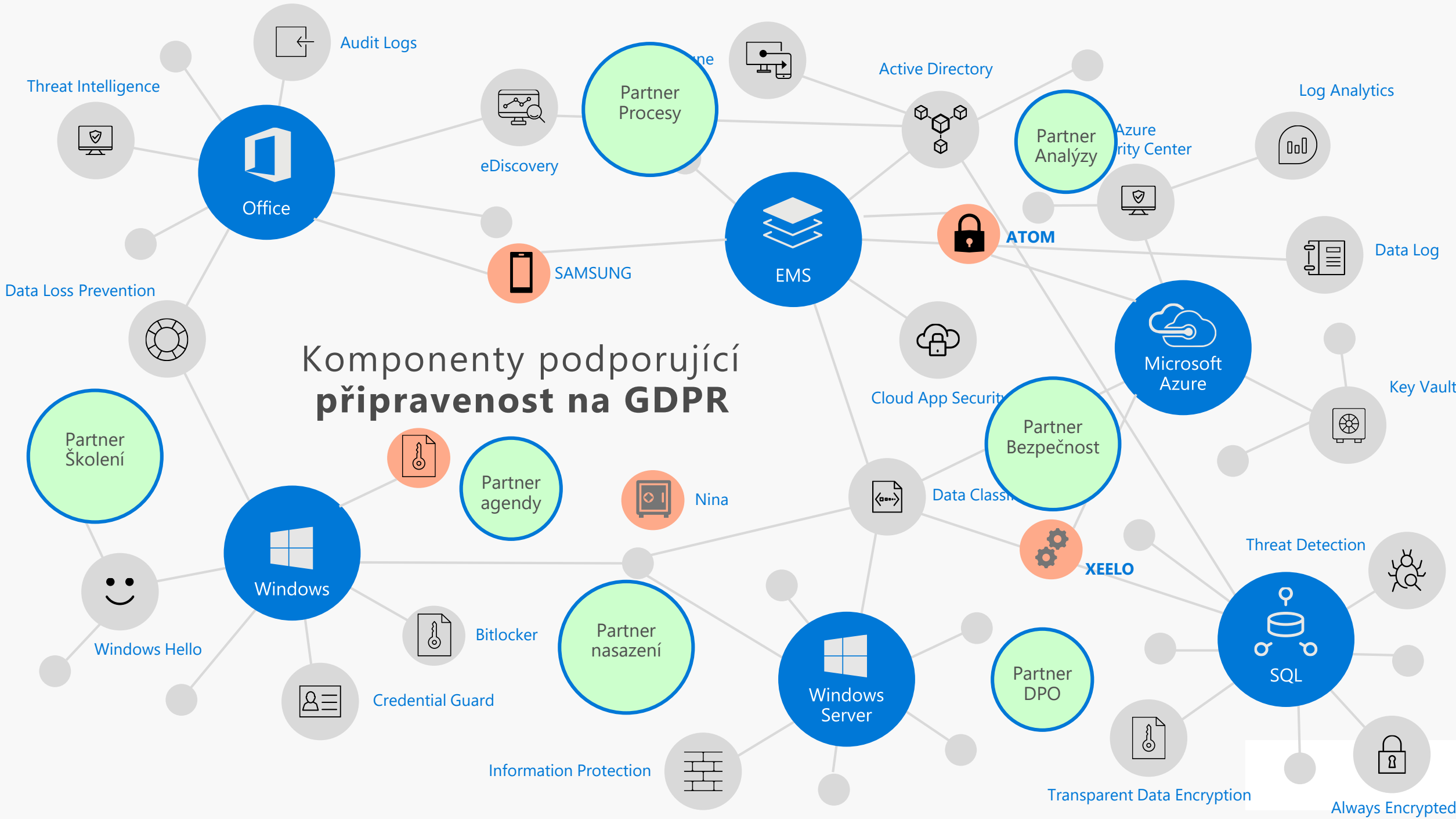
- **Windows Phone, iOS, Android**
- Zabezpečení mobilních zařízení proti neoprávněnému přístupu – Šifrování, PIN
- Snížení možnosti zneužití přístupu nebo sdílení hesla pomocí multifaktorové autentizaci pro přístup k firemním aplikacím
- Vymazání obsahu zařízení v případě odcizení nebo ztráty
 - Kompletní smazání
 - Selektivní smazání business dat
 - V kombinaci s HW zabezpečením zabránění dalšímu použití – *například pomocí Samsung Knox*



Komplexní zajištění Microsoft 365

Kombinace Windows, Office 365 a EMS

- **Ochrana koncových zařízení** před odcizením informací
- **Zajištění před neoprávněným přístupem** k zařízení a aplikacím s osobními údaji
- **Ochrana před hroby útoků** a odcizení dat v síti
- **Ochrana dokumentů a e-mailů** s osobními informacemi šifrováním
- Aplikace **Office pro bezpečnou** a efektivní **produktivitu**
- **Certifikované** cloudové **prostředí** pro e-maily a dokumenty
- **Kompletní licenční zajištění** Windows a Office 365 jako služby včetně zjednodušení správy licencí
- **Stále aktuální** prostředí z pozice bezpečnosti i funkcí



Co si tedy mohu pořídit za služby

Měsíční nebo roční předplatné na uživatele, ušetříte za servery

Podnikatelé a malé společnosti s minimem osobních dat

- **Office 365 Business Premium** – bezpečnost cloudu
- **Microsoft 365 Business** – O365 + Win10 + mobily + všechny dokumenty

Zabezpečení a platnost dokumentů – všechny dokumenty

- **Azure Information Protection** P1 nebo P2

Větší společnosti, vyhledávání dat, platnost dokumentů

- **Office 365 E3, Microsoft 365 E3** – O365 + Win10 + mobilní zař.
- **EMS** pro lokálních dokumenty + mobilů + sdílené cloudové služby

Velké společnosti, vysoká potřeba zabezpečení, velké zpracování os. Údajů

- **Microsoft 365 E5**

Zdroje k GDPR:



Microsoft Corp hlavní stránka
microsoft.com/GDPR

Online Services Terms
[Online Services Terms Download](#)

Microsoft Trust Center
microsoft.com/trust

Service Trust Platform – podklady k certifikacím, auditu
aka.ms/STP (requires log-in, NDA level)

Prezentace a zdroje v češtině:
aka.ms/jaknaGDPR

Partnerské stránky
Aka.ms/gdprpartners

GDPR Compliance Demo
<http://www.microsoftgdprscenarios.com/en-us/databreach>

Office 365 Information Protection for GDPR
<https://docs.microsoft.com/en-us/office365/enterprise/office-365-information-protection-for-gdpr>

Děkujeme Vám za pozornost

V případě dotazů kontaktujte
prosmb@microsoft.com

Příště uvidíte:

- *Možnosti cloudových služeb pro zabezpečení malých i velkých organizací*
- *Představení aplikačních řešení pro GDPR*