Microsoft

Využití cloudových služeb Microsoft pro zajištění podpory GDPR v organizacích

Petr Klement, Microsoft

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

GDPR
a zpracování osobních údajů

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

Organizační a technická opatření

- Osobní údaje by měly být zpracovávány způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění neoprávněnému přístupu k osobním údajům a k zařízení používanému k jejich zpracování nebo jejich neoprávněnému použití.
- Není-li porušení zabezpečení osobních údajů řešeno náležitě a včas, může to fyzickým osobám způsobit fyzickou, hmotnou či nehmotnou újmu, jako je ztráta kontroly nad jejich osobními údaji nebo omezení jejich práv, diskriminace, krádež nebo zneužití identity, finanční ztráta…
- Mělo by být zjištěno, zda byla zavedena veškerá vhodná technická a organizační opatření, aby se okamžitě stanovilo, zda došlo k porušení zabezpečení osobních údajů, a aby byly dozorový úřad a subjekt údajů neprodleně informovány.
- Jakmile se tedy správce o porušení zabezpečení osobních údajů dozví, měl by je bez zbytečného odkladu, a je-li to možné, do 72 hodin poté, co se o něm dozvěděl, ohlásit příslušnému dozorovému úřadu, ledaže může v souladu se zásadou odpovědnosti doložit, že je nepravděpodobné, že by dané porušení zabezpečení osobních údajů mělo za následek riziko pro práva a svobody fyzických osob.
- Při vytváření podrobných pravidel týkajících se formátu a postupů ohlašování případů porušení zabezpečení osobních údajů by měly být náležitě zohledněny okolnosti porušení, včetně otázky, zda byly osobní údaje chráněny vhodnými technickými opatřeními, jež pravděpodobnost zneužití totožnosti a jiných forem zneužívání účinně omezují…

Cesta, jak se stát a zůstat v souladu s **GDPR**

25. květnem 2018 to nekončí. Naopak začíná. Ujistěte se, že máte pokryty všechny potřebné procesy,
aby vás v budoucnu nic nepřekvapilo.

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

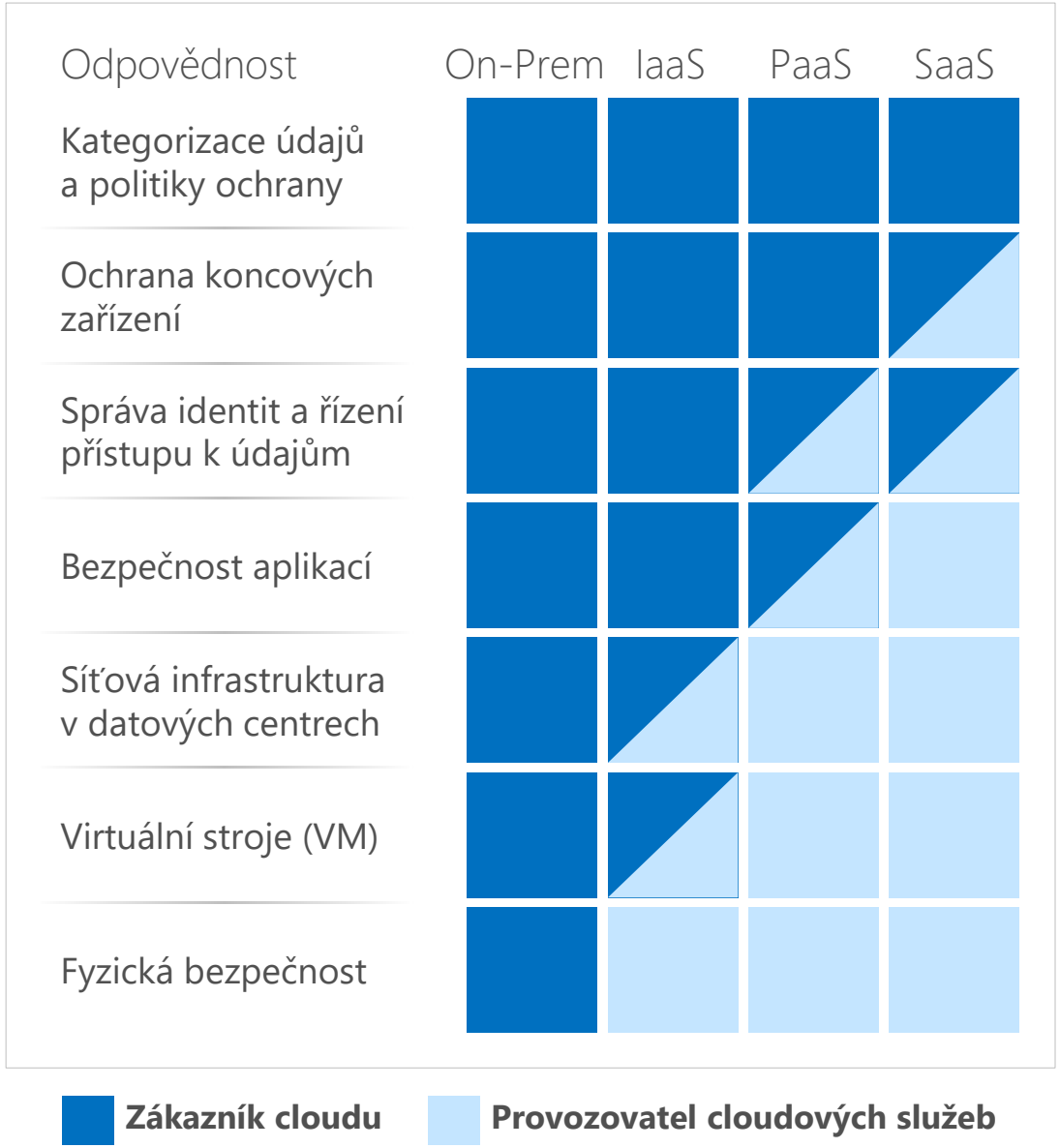
Sdílené řízení rizik

Správa identit a řízení přístupu k údajům

Řízení rizik na straně Zpracovatele

Fyzická bezpečnost a infrastruktura datových center

[Shared responsibility](#) – Microsoft whitepaper



GDPR a Microsoft
Technická a organizační opatření

Kde všude leží osobní údaje?

Servery a úložiště

- Aplikace
- Databáze
- Složky
- E-maily
- Kontakty
- Logy
- Dokumenty
- Zálohy
- Archivy
- Virtuály
- Weby

Notebooky, stanice

- Dokumenty
- E-maily
- Kontakty
- Aplikace
- Cookies

Mobil / tablet

- E-maily
- Dokumenty
- Cookies
- Aplikace

Cloudové služby

- Aplikace
- E-maily
- Dokumenty
- Webshopy
- Sociální sítě

Jinde v IT

- Zálohy
- Archivy
- Externí disky
- Síťové prvky
- Kamery
- …ky

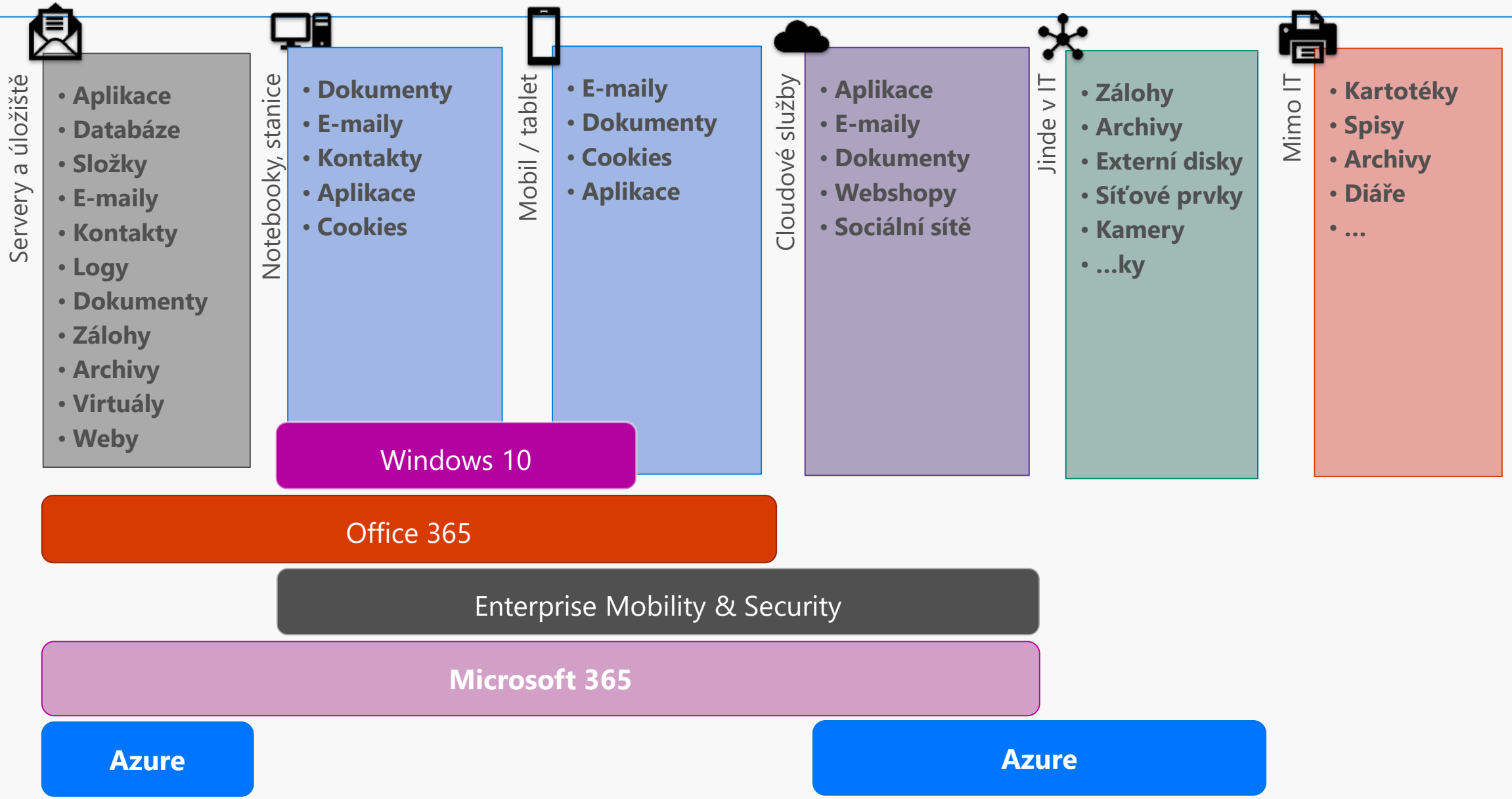
Mimo IT

- Kartotéky
- Spisy
- Archivy
- Diáře
- …

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

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.

Zdroj: ISO/IEC 29134:2017 (PIA Guidelines), publikováno 1 Jun 2017

Čl. 28 odst.1: ...správce využije **pouze ty zpracovatele**, kteří poskytují **dostatečné záruky zavedení vhodných technických a organizačních opatření** tak, aby dané zpracování splňovalo požadavky tohoto nařízení...

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 audity –** viz dále

Rozsah služeb viz Smluvní závazky zpracovatele

- Office 365, Azure Core, Dynamics Core, Cloud App Security, Intune, Business Application Platform Core

Služby pro koncové uživatele - consumer

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

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

Osobní informace E-maily a dokumenty

- **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***
- **Prokázání souladu a monitorování činností** zpracování pomocí *Office 365 Compliance Manager a auditních logů*
- **Splnění informační povinnosti** pomocí transportních pravidel v *Exchange Online*
- Možnosti **vytvoření agend** spojených se zajištěním výkonu práv subjektů – *Activity Hub pro O365, workflow pro Sharepoint Online, Azure*

Search
Home
Add GDPR Request
Add GDPR Event/Incident
GDPR Hierarchy
GDPR Tasks
Events
Requests
Recycle bin
Edit

GI

GDPR Activity Hub

Public group

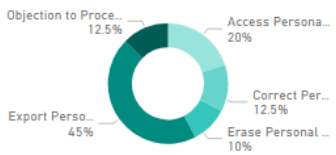
New

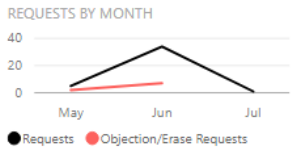
Published 6/27/2017 | Edit

Data Requests

1/3/2017 – 11/15/2017

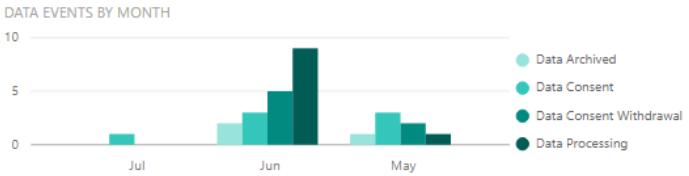
8	5	18	5	4
Access	Correct	Export	Objection	Erase





Data Events

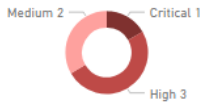
7	43 %	10...	10	3
Data Consent	% Sensitive Data	% Consent Withdrawal	Data Processing	Data Archived

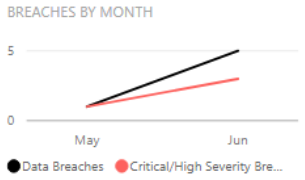


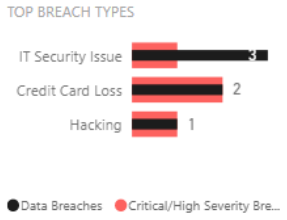
Data Breaches

Open | Solved

6	67 %
Data Breaches	% Critical/High Severity Breaches

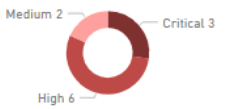


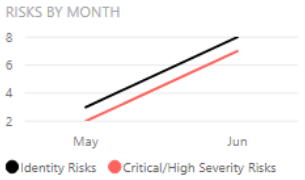


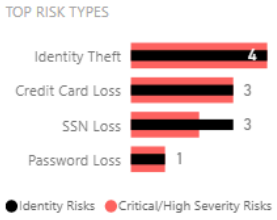


Identity Risks

11	81.8%
Identity Risks	% Critical/High Severity Risks

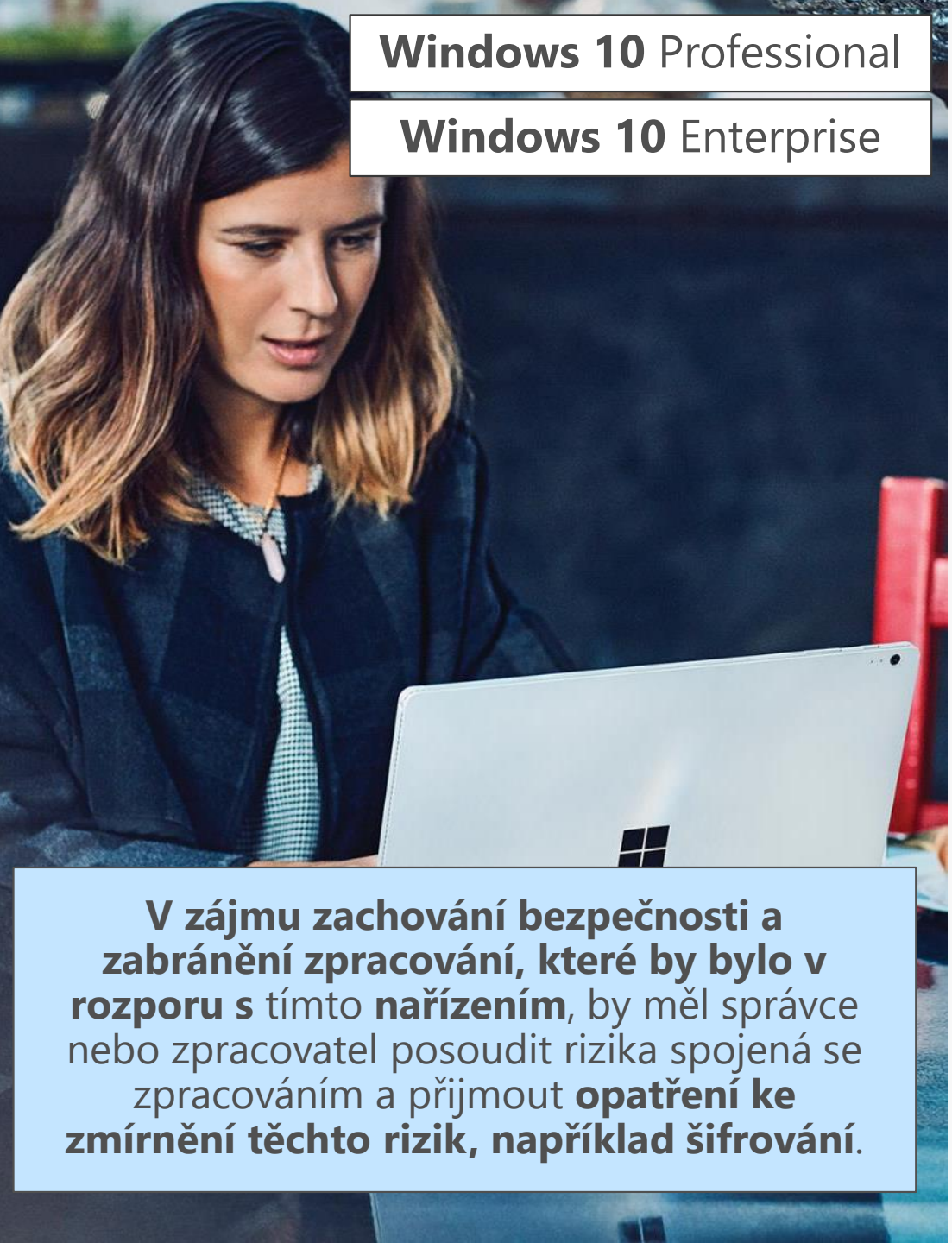






E-maily a dokumenty mimo Office 365

- **Prohledání 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…



Windows 10 Professional

Windows 10 Enterprise

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**.

Ochrana koncových stanic

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.

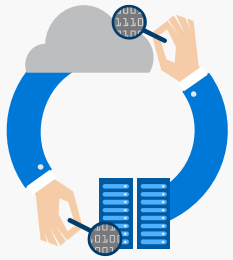
Zabezpečené informací při odcizení nebo ztrátě

- **Firemní a informace osobní data** na zařízeních a uložištích zabezpečená 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**

Office 365

Enterprise Mobility & Security

Osobní údaje by měly být zpracovávány způsobem, který zaručí náležitou bezpečnost a důvěrnost těchto údajů, mimo jiné za účelem zabránění **neoprávněnému přístupu** k osobním údajům a **k zařízení** používanému k jejich zpracování nebo jejich neoprávněnému použití



Ochrana mobilů a tabletů

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*

Microsoft 365 Business

Microsoft 365 E3 , E5

Komplexní zajištění

Office 365, Windows10 a EMS

- **Ochrana koncových zařízení** před odcizením informací
- **Zajištění před neoprávněným přístupem** k zařízení a aplikacím s osobními údaji
- **Ochrana před hrobami 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

S přihlédnutím ke stavu techniky, nákladům … …**provedou správce a zpracovatel vhodná technická a organizační opatření**, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně … **schopnosti zajistit** neustálou důvěrnost**, integritu, dostupnost** a odolnost systémů a služeb zpracování

Aplikace důvěrnost, integrita

Azure IaaS pro stávající aplikace

- Aplikace využívající **nedostatečně** technicky a organizačně **zajištěnou infrastrukturu**
- Přenesení části požadavků k naplnění **zavedení vhodných technických a organizačních opatření** na zajištění ochrany práv subjektu údajů na zpracovatele
- **Zálohování** a Disaster **recovery**

Azure PaaS pro nové a redesignované aplikace

- **Minimalizace vstupních investic** do HW vybavení a a **okamžitá dostupnost** pro vývoj a provoz nových aplikací, splňujících požadavky GDPR
- **Využití** bezpečnostních prvků **databázových technologií** Microsoft SQL Server, Azure SQL, CosmoDB …
- **Bezpečné prostředí provozu** aplikací, splňujících požadavky GDPR
- **Vývoj a provoz aplikací** spojených se zajištěním **výkonu práv subjektů**

S přihlédnutím ke stavu techniky, nákladům …
…**provedou správce a zpracovatel vhodná technická a organizační opatření**, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně …
schopnosti zajistit neustálou **důvěrnost, integritu**, dostupnost a **odolnost systémů a služeb** zpracování

Nástroje

Dostupnost, odolnost, kontrola

Předcházení bezpečnostním incidentům

- Integrace systémů do jednoho globálního pohledu ze všech komponent on-prem i cloudu – sítě, servery, identity, SIEM
- Doporučení pro zabezpečení monitorované infrastruktury napříč platformami – Windows, Linux, OpenStack, Vmware…
- Zabezpečení proti neomezenému přístupu administrátora
- Analýza hrozeb na základě podezřelých aktivit uživatele
  - V rámci AD pomocí *Advanced Threat Analytics*
  - V rámci cloudových služebv pomocí *Cloud Apps Security*

Detekce a zvládání incidentů – Security as a Service

- Notifikace o incidentech (SMS, e-mail, push, dashboard, mobilní aplikace), propojení se systémy pro vyhodnocování v reálném čase (SIEM…)
- Zpětné dohledání incidentů po dobu až 24 měsíců s neomezeným prostředky – úložiště, výkon, analýzy…
- Vyhledání události, incidentu, spojených s konktrétním uživatelem nrbo prostředkem

Veškerou újmu, která může osobám vzniknout v důsledku zpracování, které porušuje toto nařízení, **by měl nahradit správce nebo zpracovatel**.

S cílem posílit prosazování pravidel tohoto nařízení **by za jakékoliv jeho porušení měly být uloženy sankce** včetně správních pokut…

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

Bezpečnost pro každého nejen kvůli GDPR

1. Zašifrujte si svůj notebook pomocí BitLockeru

Pokud je nepravděpodobné riziko zneužití, nemusíte informovat regulátora, ani subjekty údajů.

2. Nastavte si šifrování a PIN pro mobilní telefon

Pokud je nepravděpodobné riziko zneužití, nemusíte informovat regulátora, ani subjekty údajů.

3. Přesuňte svůj e-mail do Office 365

Ochrana proti spamu a malwaru , vyhledávání osobních informace napříč Office 365 díky eDiscovery. Smluvní závazky Office 365 pro GDPR.

4. Ukládejte dokumenty na OneDrive for Business v Office 365

Bezpečné sdílení dokumentů uvnitř i mimo firmu, automatické ukládání z aplikací Office, omezení kopií dokumentů v přílohách a hlavně automatická záloha. Smluvní závazky Office 365 pro GDPR.

5. Chraňte citlivé dokumenty pomocí Information protection

Dokumenty jsou šifrované, otevřou je pouze ověření uživatelé, dokument je možné zneplatnit v případě neaktuálnosti osobních informací a eliminovat riziko úniku informací.

6. Udržujte své zařízení aktualizované

Pouze aktualizované systémy mohou být bezpečné a Microsoft pravidelně vydává bezpečnostní aktualizace, které zamezují napadnutí počítače s Win10 a Office365 novými typy útoků.

7. Zvýšení lokálního zabezpečení přesunem aplikací do Azure

Využití infrastruktury v Azure sníží možnost odcizení nebo napadení serverů s fyzickým přístupem

Co si tedy mohu pořídit za služby

Předplatné na uživatele, úspora za HW, nasazení a zabezpečení

Podnikatelé a malé společnosti s minimem osobních dat

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

Zabezpečení a platnost dokumentů – všechny dokumenty

- Azure Information Protection

Větší společnosti a podniky, maximální ochrana, nastavení platnosi dokumentů

- Office 365 E3, Microsoft 365 E3 – O365 + Win10 + mobilní zař.
- EMS pro lokálních dokumenty + mobilů + sdílené cloudové služby
- Microsoft 365 E3, E5 – Win10 ENT, O365, kompletní sada EMS

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, audity
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


Microsoft
Děkuji Vám za pozornost
This presentation is intended to provide an overview of GDPR and is not a definitive statement of the law.