Regulace, cloud a egovernment mohou jít ruku v ruce

Zdeněk Jiříček, National Technology Officer
Microsoft CZ/SK

Pohled regulátora na bezpečnost a obezřetnost IS

Povinná osoba – jistota souladu s regulatorními požadavky

Co to je „přístup založený na riziku“

(r. 2000): Správce a zpracovatel jsou povinni přijmout taková opatření, aby nemohlo dojít k neoprávněnému nebo nahodilému přístupu k osobním údajům….

(r. 2006): Orgány veřejné správy uplatňují opatření odpovídající bezpečnostním požadavkům na zajištění důvěrnosti, integrity a dostupnosti informací zpracovávaných v informačních systémech veřejné správy.

(r. 2014): Orgány a osoby uvedené v ..... jsou povinny zavést a provádět bezpečnostní opatření v rozsahu nezbytném pro zajištění kybernetické bezpečnosti informačního systému....

GDPR článek 32 – Zabezpečení zpracování

- (1) S přihlédnutím ke stavu techniky... povaze... rozsahu... a k různě závažným rizikům pro práva fyz. osob, zavedou správce a zpracovatel **vhodná tech/org. bezp. opatření**.... odpovídající danému **riziku**,.. včetně:
  - a) případné **pseudonymizace** a **šifrování** osobních údajů;
  - b) schopnosti zajistit **neustálou důvěrnost**, **integritu**, **dostupnost** a **odolnost** systémů a služeb zpracování;
  - c) …**obnovit dostupnost** osobních údajů…**včas** v případě…technických incidentů;
  - d) …**pravidelného** testování…a **hodnocení účinnosti** zavedených…**opatření**…
- (2) … **zohlednit rizika**… náhodného **zničení**, **ztráty**, **pozměňování**, neoprávněného **zpřístupnění**… osobních údajů

Rozdělení odpovědností Správce - Zpracovatel

Řízení rizik na straně Správce

Kategorizace údajů a stanovení politik ochrany

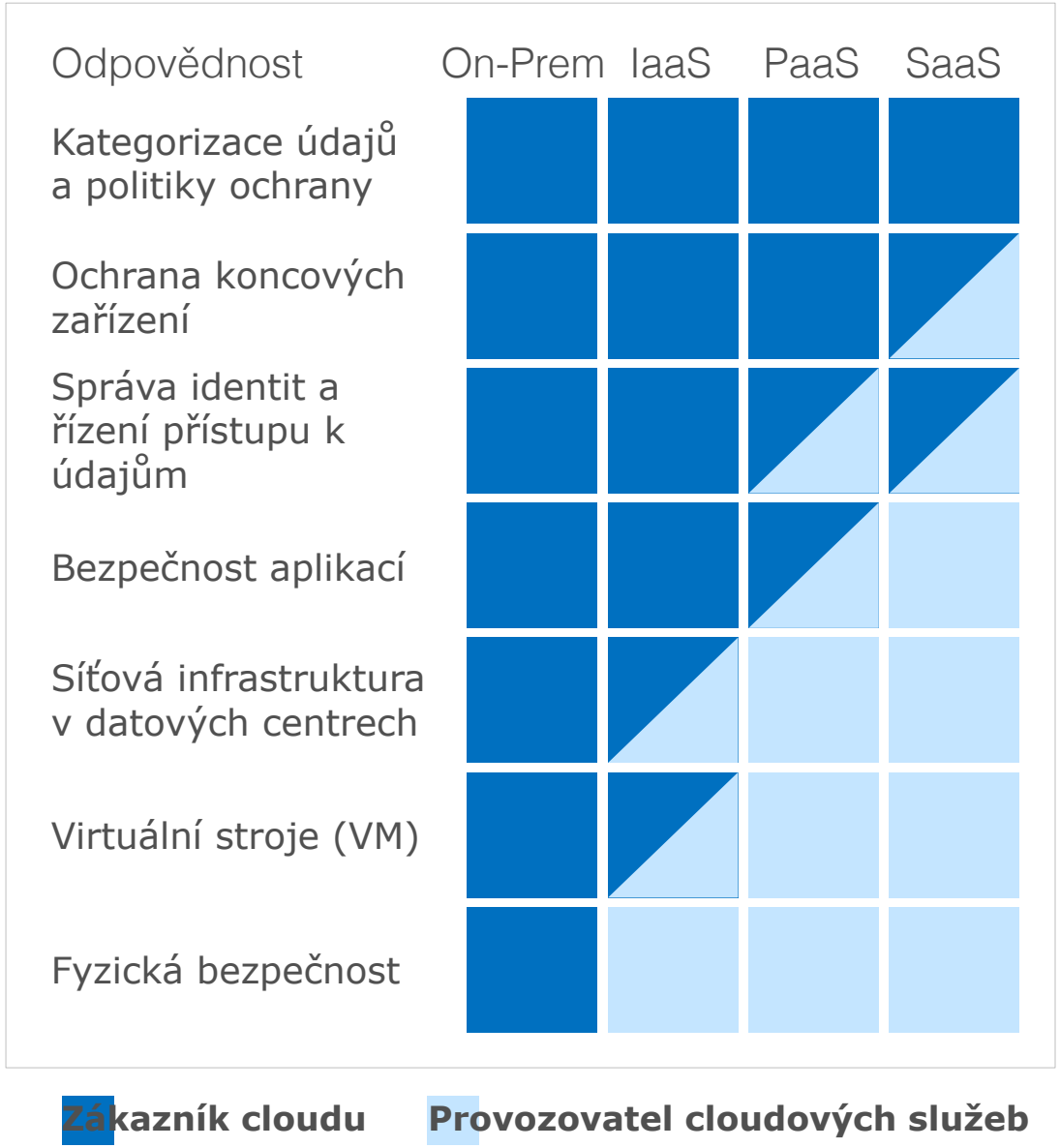
řízení rizik

ntit a řízení přístupu k údajům

izik na straně Zpracovatele

zpečnost a infrastruktura datových center

[Shared responsibility](#) – Microsoft whitepaper



Microsoft cloud a soulad s GDPR

Požadavek	Řešení
Smluvní podmínky dle čl. 28	**Microsoft „Podmínky pro služby online“ (OST)** od září 2017: Standardně nová příloha č. 4 – řeší explicitně soulad s články 28, 32 a 33 GDPR. Dále: „Podmínky ochrany osobních údajů a zabezpečení“ dle GDPR (str. 8 a dále)
Zabezpečení zpracování – čl. 32	OST – Příloha 4 GDPR, dále část „Zabezpečení“ Bezp. opatření, průmyslové certifikace / standardy a auditní zprávy – vše zahrnuto v OST
Podklady k bezp. opatřením	Rozcestník: Trust Center www.microsoft.com/trust Celé auditní zprávy a dokumenty jsou na Service Trust Platform (www.aka.ms/STP)
Analýza rizik a DPIA	Vzorové analýzy rizik zpracování v cloudu pro Azure a Office 365 zdarma k dispozici zákazníkům a partnerům
Kodexy chování a osvědčení čl. 40-43	Microsoft bude adoptovat kodexy chování a osvědčení (certifikace), jakmile budou vyhlášeny dozorovým úřadem (ÚOOÚ) – údajně po termínu účinnosti 25/6/18

Kde najdeme Security & Privacy controls

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

str. 12 – 14: seznam bezp. opatření ve struktuře ISO 27001:2013, závazek pokračovat s 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)

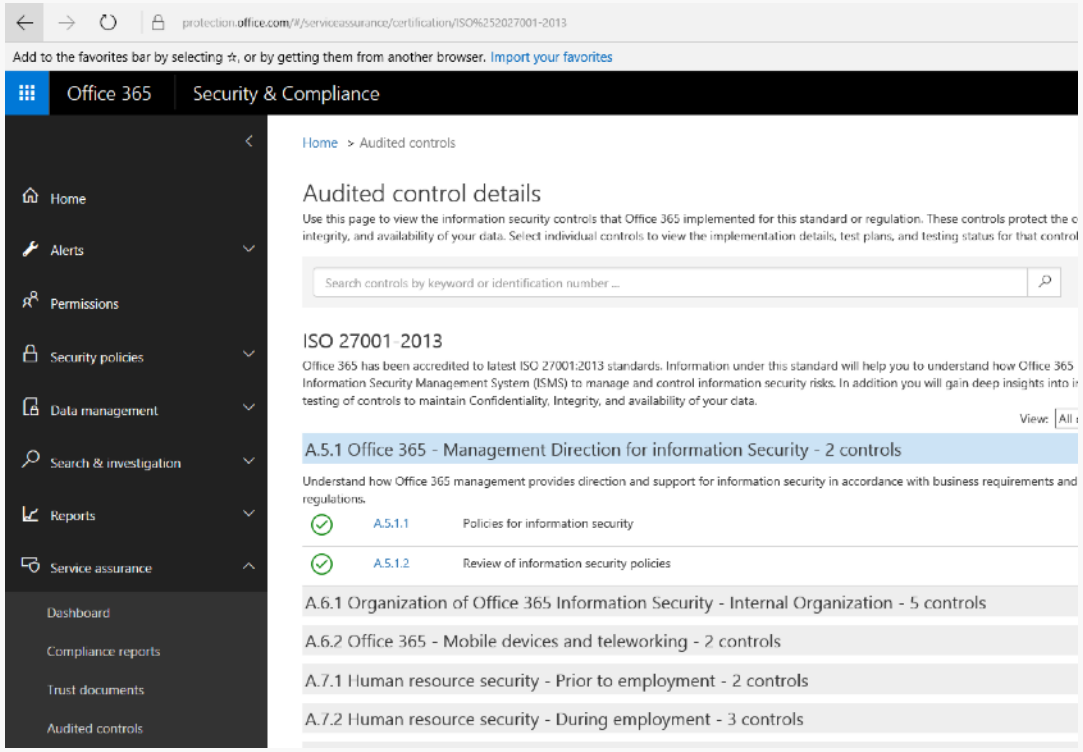
také aka.ms/STP

Repository podkladů k certifikacím:

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

O365 Service Assurance

https://protection.office.com



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**

„Úrovně dopadů“ = vstup pro posouzení rizik

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

Zanedbatelný	Omezený	Vysoký	Kritický
Telefonní seznam	Vyúčtování služebních cest	Správní delikty	Zdravotnická dokumentace
Seznam účastníků konference (pokud něco neprozrazuje!)	Fotografie na ID karty	Daňová přiznání	Registry s citlivými osobními údaji
E-mailové adresy	Logy s IP adresami	Informace s výsledkem psychologického testu	Kompromitující materiály na jednotlivce
Patičky e-mailů	Zdravotní způsobilost	Kárná řízení	
	CV interních zaměstnanců	Foto s citlivým obsahem	
Podráždění jednotlivce, likvidace nevyžádané pošty, potřeba znovu vyplnit formulář po ztrátě dat	Potíže, které však lze poměrně snadno překonat: Zvýšené náklady, odmítnutí některé z komerčních služeb, obavy, nedorozumění	Vážné potíže. Diskriminace: blacklisting většinou bank. Vznik vysokého finančního závazku. Ztráta zaměstnání. Vyloučení v rodině, v místě bydliště.	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

Příklad výpočtu inherentního a zbytkového rizika

Vzorec: Riziko = max(C-I-A-T) + hrozba + zranitelnost -2

Typ aktiv	Aktivum	Hrozba	Zranitelnost	Částečná úroveň rizika				Riziko	Snížení hrozby		Snížení zranit.		Zbytkové riziko
				C	I	A	T		MAX	Hodnota	MAX	Hodnota	
Datová aktiva													
	Uložená data	Zneužití práv (neoprávněná akce obsluhy)	Zneužití oprávnění pracovníky správce	3	4	2	3	8	2	2	4	4	8
	Uložená data	Zneužití práv (neoprávněná akce obsluhy)	Zneužití oprávnění pracovníky poskytovatele	3	4	2	3	8	2	2	4	1	5
	Uložená data	Nesprávné řízení bezpečnosti	Nesprávné vyhodnocení SLA	3	4	2	3	7	1	1	4	4	7
	Uložená data	Nesprávné řízení bezpečnosti	Regulatorní nesoulad způsobený poskytovatelem	3	4	2	3	7	1	1	4	2	5
Služby													
	Služba SharePoint Online	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	Zneužití přístupových údajů a klíčů	3	4	2		9	3	2	4	1	5
	Služba SharePoint Online	Neoprávněný přístup k aktivu cizími osobami	Zneužití přístupových údajů a klíčů (útok hackerů)	3	4	2		10	4	2	4	1	5
	Služba SharePoint Online	Zneužití systémových zdrojů	Obecná zranitelnost u správce	3	4	2		7	1	1	4	4	7
	Služba SharePoint Online	Zavedení škodlivého software	Obecná zranitelnost ze strany správce	3	4	2		9	3	2	4	1	5
	Služba SharePoint Online	Popření	Obecná zranitelnost	3	4	2		8	2	1	4	2	5
	Služba SharePoint Online	Napadení komunikace	Obecná zranitelnost	3	4	2		8	2	2	4	1	5
	Služba SharePoint Online	Přerušení komunikace	Obecná zranitelnost			2		6	2	2	4	3	5
	Služba SharePoint Online	Kybernetický útok z komunikační sítě	Obecná zranitelnost (útok hackerů)	3	4	2		10	4	2	4	1	5
	Služba SharePoint Online	Selhání hardware nebo média	Obecná zranitelnost u poskytovatele		4	2		8	2	1	4	1	4
	Služba SharePoint Online	Selhání software	Obecná zranitelnost u poskytovatele	3	4	2		8	2	1	4	1	4
	Služba SharePoint Online	Selhání podpory prostředí (vč. přírodních katastrof)	Obecná zranitelnost u poskytovatele			2		6	2	1	4	1	2
	Služba SharePoint Online	Selhání údržby	Obecná zranitelnost u poskytovatele	3	4	2		8	2	1	4	1	4
	Služba SharePoint Online	Chyba uživatele	Obecná zranitelnost u správce	3	4	2		8	2	2	4	3	7
	Služba SharePoint Online	Prozrazení informaci z vyřazené komponenty nebo média	Obecná zranitelnost	3				7	2	1	4	2	4
	Služba SharePoint Online	Úmyslné poškození interními pracovníky	Obecná zranitelnost (vandalismus)			2		5	1	1	4	2	3
	Služba SharePoint Online	Úmyslné poškození externími pracovníky	Obecná zranitelnost			2		5	1	1	4	1	2
	Služba SharePoint Online	Nesprávné řízení bezpečnosti	Obecná zranitelnost u poskytovatele	3	4	2		8	2	1	4	1	4
	Služba Azure AD	Neoprávněný přístup k aktivu interními pracovníky nebo dodavateli služeb	Zneužití přístupových údajů a klíčů	2	4	2		9	3	2	4	1	5
	Služba Azure AD	Neoprávněný přístup k aktivu cizími osobami	Zneužití přístupových údajů a klíčů (útok hackerů)	2	4	2		10	4	2	4	1	5

Příklad uplatnění opatření na inherentní riziko

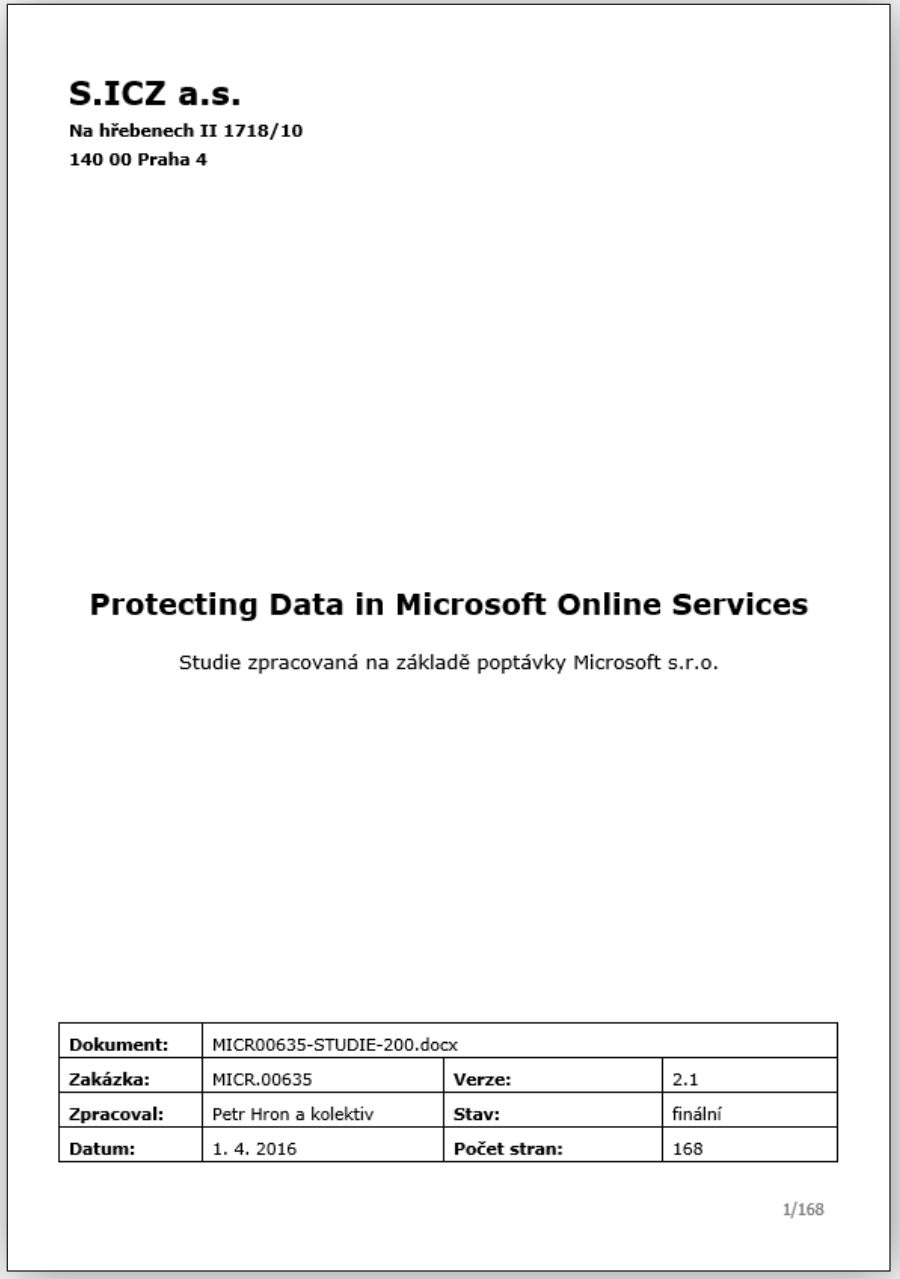
Služby			
SharePoint Online / Neopráv. přístup intern. prac. / Obecná	9	5	I-9-0 Řízení přístupu osob II-3-0 Nástroj pro ověřování identity uživatelů II-4-0 Nástroj pro řízení přístupových oprávnění II-6-0 Nástroj pro zaznamenávání činnosti II-8-0 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí II-10-1 Kryptografické prostředky ochrana dat v klidu) II-10-2 Kryptografické prostředky ochrana dat při přenosu)
SharePoint Online / Neopráv. přístup ext. prac. / Obecná	10	5	II-3-0 Nástroj pro ověřování identity uživatelů II-4-0 Nástroj pro řízení přístupových oprávnění II-6-0 Nástroj pro zaznamenávání činnosti II-8-0 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí II-10-1 Kryptografické prostředky ochrana dat v klidu) II-10-2 Kryptografické prostředky ochrana dat při přenosu)
SharePoint Online / Kyber. útok / Obecná	10	5	I-8-0 Řízení provozu a komunikací I-10-0 Akvizice, vývoj a údržba I-11-0 Zvládání bezpečnostních událostí a bezpečnostních incidentů II-2-0 Nástroj pro ochranu integrity komunikačních sítí II-6-0 Nástroj pro zaznamenávání činnosti II-7-0 Nástroj pro detekci kybernetických bezpečnostních událostí II-8-0 Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí II-9-0 Aplikační bezpečnost II-10-1 Kryptografické prostředky ochrana dat v klidu)

Katalog opatření, která jsou k dispozici v Office 365

Zabezpečení dat

Jak splnit požadavky vyhlášky č. 316/2014 Sb (VoKB)

- pro všechny úrovně hodnocení aktiv (dle Přílohy 1 vyhlášky)
- bezpečnostní opatření v rámci Microsoft Azure a Office 365
- studie S.ICZ a.s. jako podklad pro analýzu rizik a zabezpečení dat



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

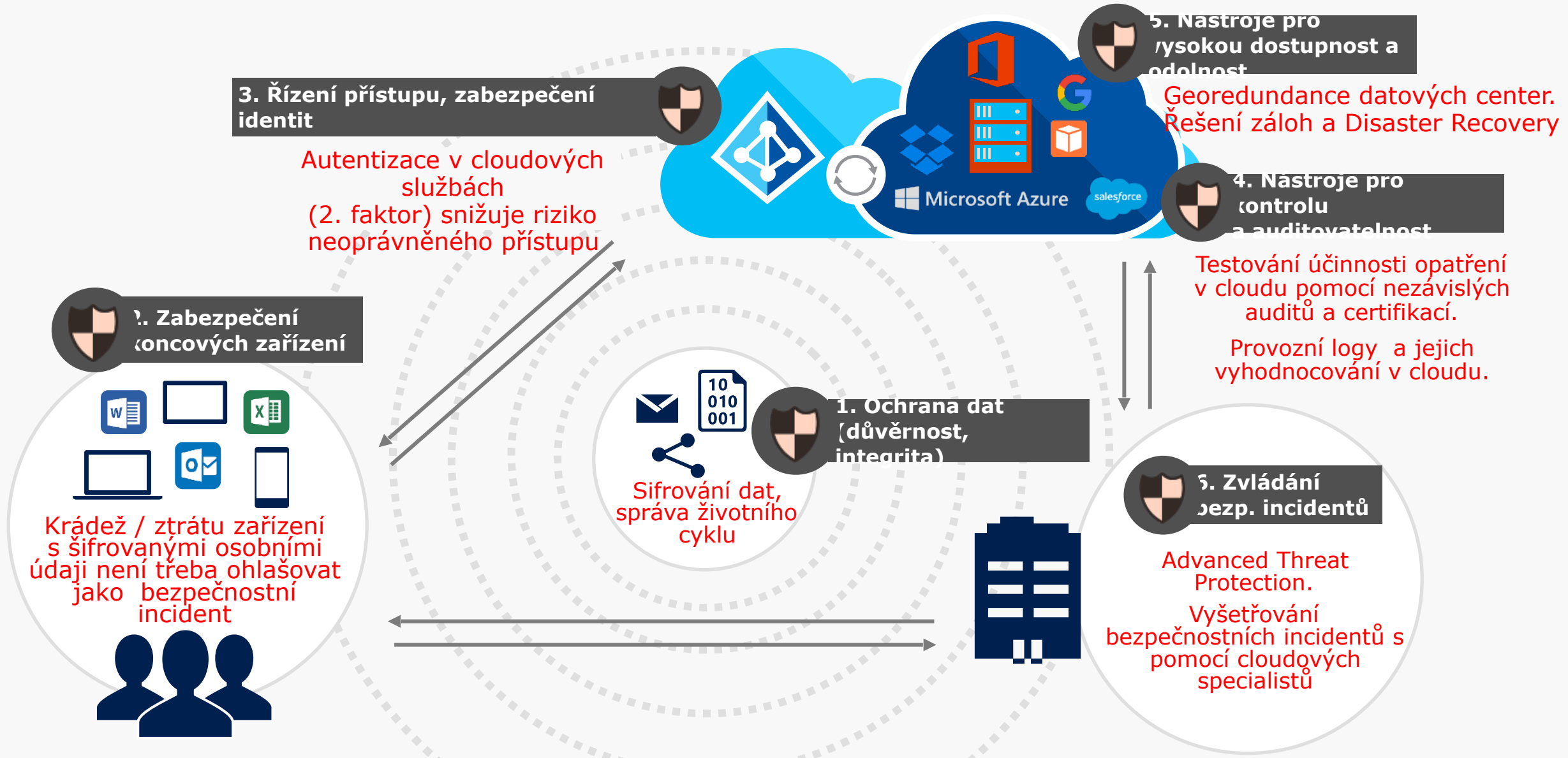
Protecting Data in Microsoft Online Services

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

Dokument:	MICR00635-STUDIE-200.docx		
Zakázka:	MICR.00635	**Verze:**	2.1
Zpracoval:	Petr Hron a kolektiv	**Stav:**	finální
Datum:	1. 4. 2016	**Počet stran:**	168

1/168

Přenesení části odpovědnosti na zpracovatele



Řešení podporující **připravenost na GDPR**

Zpracování běžných osobních údajů bez DPIA

Technická a organizační opatření v cloudu Microsoft

- Zabezpečená infrastruktura (datové centrum, konc. zařízení)
- Smluvní závazky a SLA zpracovatele

Migrace zpracování do Office 365 / Azure IaaS

Ochrana informací s osobními údaji:

- **Vyhledání** dokumentů, e-mailů, kontaktů s osobními údaji a informací na webech napříč systémem Office 365 pomocí funkce eDiscovery pověřenými osobami
- **Zabezpečení dokumentů a e-mailů** – možnost zneplatnění a omezení přístupu bez ohledu na jejich umístění, DLP, nastavení retenčních politik a analýza jejich dodržování
- **Minimalizace výskytu** stejných dokumentů s osobními údaji jejich jednoduchým sdílením a ne kopírováním pomocí e-mailových příloh – propojení s aplikacemi Office

Zpracovávání s vysokým rizikem pro subjekty údajů

potřebné DPIA

Vše ze základního scénáře

Vysoká úroveň zabezpečení infrastruktury, aplikací, uživatelů i zařízení

- Předcházení bezpečnostních incidentů a včasná reakce na incident – Security as a Service
- Zajištění koncových zařízení proti krádeži, neoprávněnému přístupu i kyber-útokům
- Monitorování rizik cloudovými nástroji
- **Funkce Azure OMS, O365 E5, Win 10 ATP, EMS, M365 E5**

Vytvoření nových aplikací a agend splňujících GDPR

- Zajištění aplikací pro podporu GDPR (evidence žádostí subjektů, mapy osobních údajů a provozní záznamy)
- Centralizace agend a osobních údajů do O365/D365
- Pseudonymizace a pokročilé šifrování údajů
- **Nové aplikace v Azure PaaS, Dynamics 365**
- **Partnerská řešení pro GDPR (KPCS Atom, Xeelo…)**

Modelové analýzy rizik a scénáře pro DPIA

- Stránky GDPR konference: www.aka.ms/jaknaGDPR
  k dispozici modelové analýzy rizik pro zákazníky (v češtině):
  - 1) Analýza rizik: **Zdravotnická dokumentace v cloudu Azure** (ICZ a.s.)
    - Znalecký posudek ústavu CETAG: adekvátní úroveň zabezpečení dle GDPR
  - 2) Analýza rizik: **Spisová služba Gordic GINIS v cloudu Azure** (RAC s.r.o.)
  - 3) **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

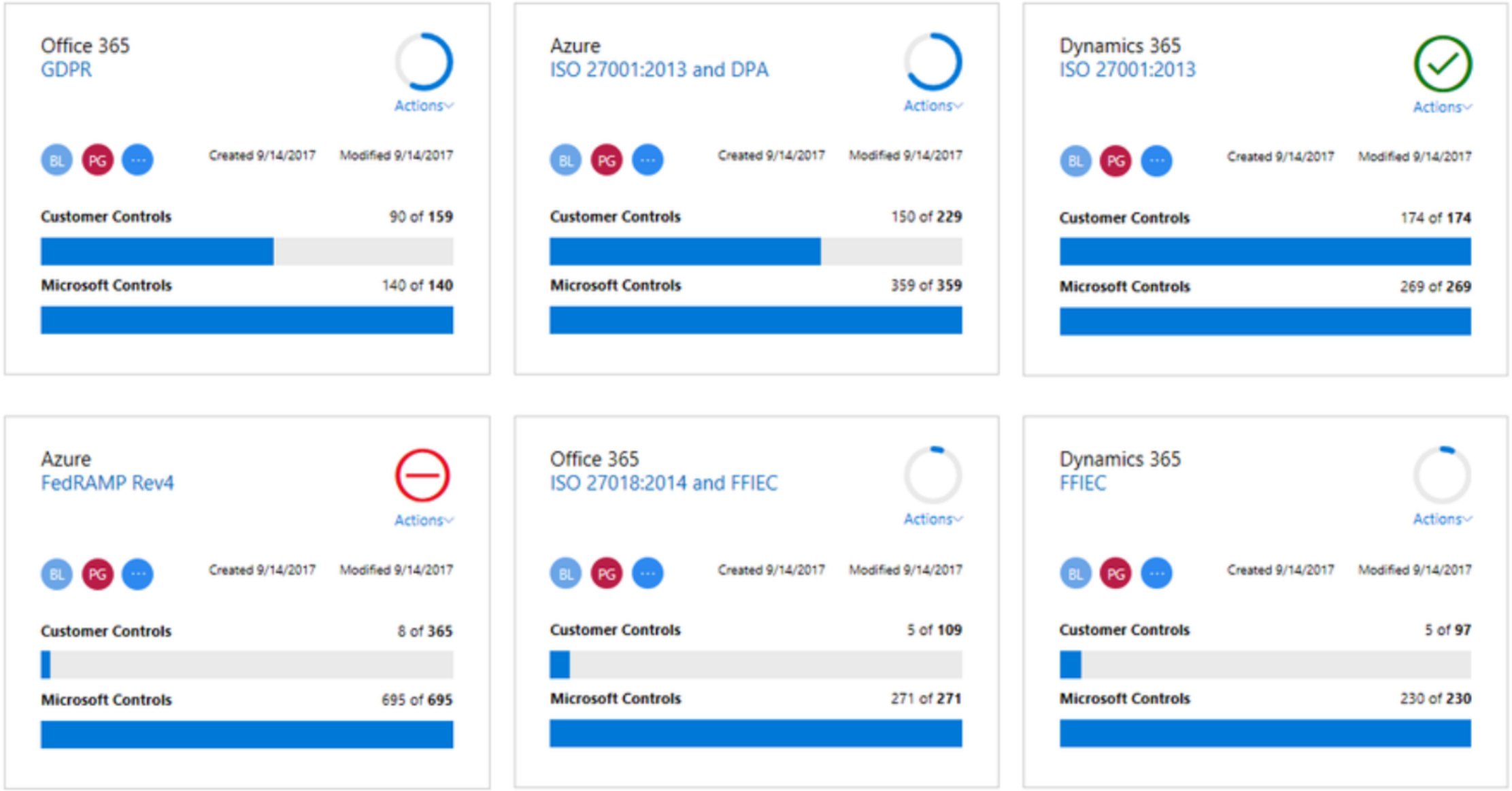
Studie zpracovaná na základě poptávky Microsoft s.r.o.

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

Microsoft Compliance Manager (Preview)

Cloudová služba - dohled nad stavem zvolených opaření v reálném čase - [blog]



Informace k souladu:

GDPR hlavní stránka:
microsoft.com/GDPR a česká verze:
www.microsoft.com/sk-sk/rethink-IT-security/GDPR

Prezentace a vzorové analýzy rizik 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)

Děkuji Vám za pozornost

Zdeněk Jiříček

zdenekj@microsoft.com

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