



# GDPR a DPIA

Gabriel Fedorko  
National Technology Officer  
Microsoft Czech&Slovak  
Slovakia





## Článok 32 – Zabezpečenie spracovania (os. údajov)

- (1) S prihliadnutím ku stavu techniky... povahe... rozsahu... a k rôznym závažným rizikám pre práva fyz. osôb, zavedú správca a spracovateľ **vhodné tech/org. bezp. opatrenia.... zodpovedajúce danému riziku**,.. včítane:
  - a) **pseudonymizácia** a **šifrovanie** osobných údajov;
  - b) schopnosť zaistiť **stálu dôvernosť, integritu, dostupnosť** a **odolnosť** systémov a služieb spracovania;
  - c) **...obnoviť dostupnosť** osobných údajov...**včas** v prípade...technických incidentov;
  - d) **...pravidelného testovania...a hodnotení účinnosti zavedených...opatrení...**
- (2) **... zohľadniť rizika... náhodného zničenia, straty, zmeny, neoprávneného sprístupnenia... osobných údajov**

# Široké portfólio certifikácií a medzinárodných štandardov

Certifikácie a požiadavková dokumentácia dostupná na Microsoft Trust Center [www.microsoft.com/trust](http://www.microsoft.com/trust)

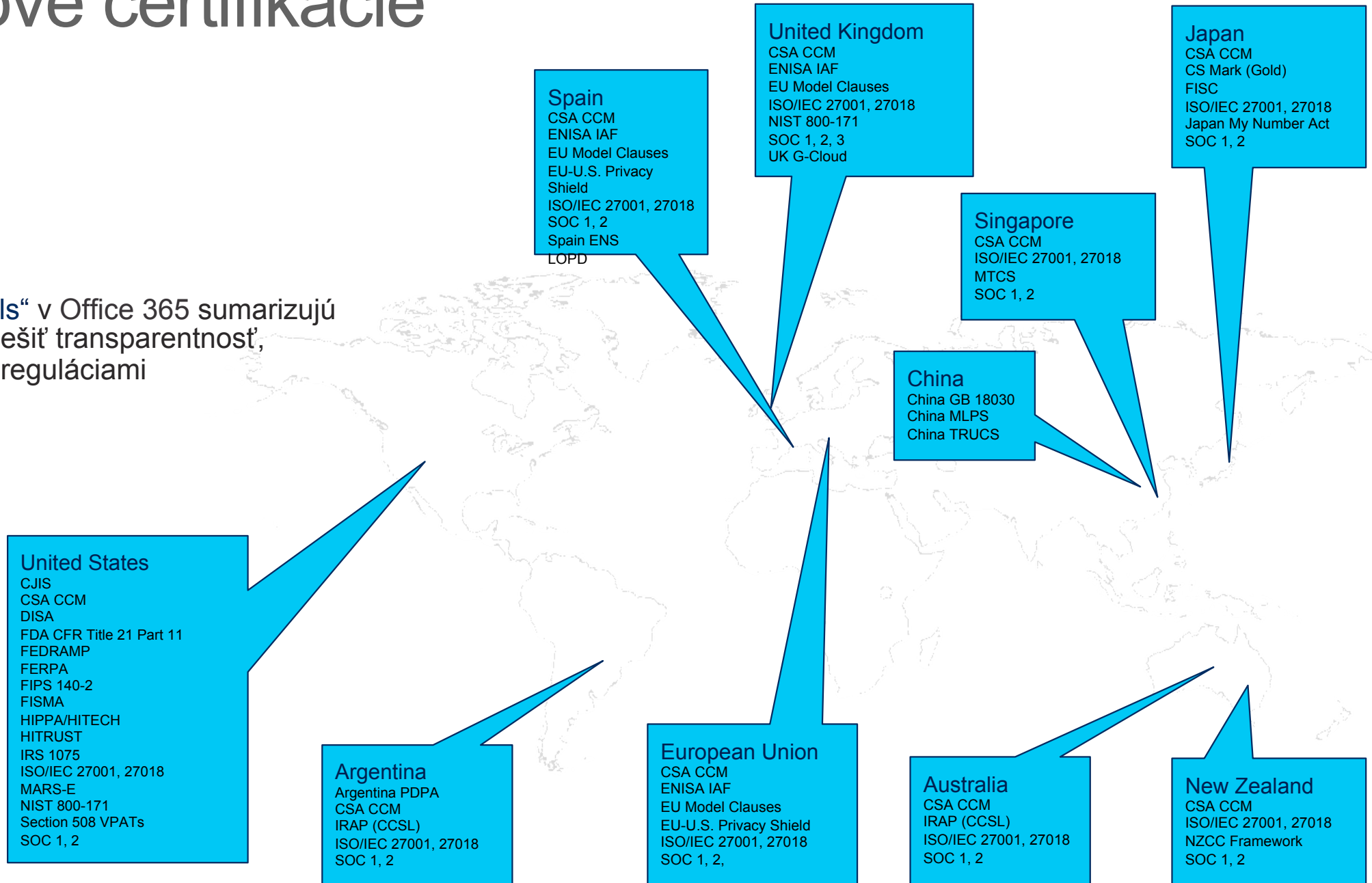
January 2017

Worldwide	 ISO 27001	 ISO 27017	 ISO 27018	 Cloud Controls Matrix	 SOC 1 (SSAE 16) Type II	 SOC 2 (AT101) Type II	 PCI DSS Level 1 *	 Content Delivery and Security Association *			
National	 HIPAA / HITECH	 European Union Model Clauses	 ENISA IAF	 EU-U.S. Privacy Shield	 Spain ENS	 Singapore MTCS Level 3	 Australian Signals Directorate	 New Zealand GCIO	 Japan Financial Services	 China MLPS*, TRUCS*, GB 18030*	
Government	 Section 508 VPAT	 United Kingdom G-Cloud	 FedRAMP JAB P-ATO	 FIPS 140-2	 21 CFR Part 11	 FERPA	 DISA Level 2	 CJIS	 IRS 1075	 FISMA	 NIST 800-171

\*Denotes Microsoft Azure-specific certifications

# Kľúčové certifikácie

Viac ako 1000 „controls“ v Office 365 sumarizujú našu skúsenosť ako riešiť transparentnosť, bezpečnosť a súlad s reguláciami





# Od analýzy rizík k DPIA (Článok 35)

- GDPR: nutné „posúdenie vplyvu“ (DPIA – Data Protection Impact Assessment) pre spracovanie údajov s vys. rizikom
- Spracovateľ: ako najlepšie vyhovieť správcovi a regulátorovi
  - **1. Modelová analýza rizík určitého typu spracovania** osobných údajov
    - Hodnotíme riziká porušenia dôvernosti, integrity a dostupnosti osobných údajov
    - Ďalej riziká súladu s regulatornými požiadavkami pre správcov
  - **2. Nastavenie adekvátnych bezp. opatrení**
  - **3. Charakteristika zostatkových rizík pre správcu**



# Vzorové „Posúdenie vplyvu“ DPIA na Office 365

- Spracovanie osobných údajov v Office 365 -vzorové scénare:
  - Osobné údaje v Exchange Online / Outlook
  - Citlivé osobné údaje v SharePoint Online
    - napr. výpis zo zdravotníckej dokumentácie
  - Telemedicína / citlivé osobné údaje cez Skype forBusiness
- Analýza rizík a návrh zmierňujúcich bezpečnostných opatrení
- Formát „posúdenie vplyvu na ochranu osobných údajov (DPIA)“
  - Navyše: popis účelu a scénare spracovania osobných údajov
  - Navyše: posúdenie potreby a primeranosti operácií spracovania

Zákazník vlastní dáta.

Nevyťahujeme zákaznicke data pre reklamné účely.

Konfigurovateľné súkromie podľa organizačných politik.

Sme advokátom zákazníkov pri ochrane ich súkromia.

Všetky naše záväzky sú súčasťou kontraktu





# Transparentnosť

Viete kde sú vase data uložené

Rozumiete tomu, kto má prístup k vašim dátam a na základe akých pravidiel.

Monitorujete stav vašich služieb v reálnom čase







# Naša bezpečnostná platforma



Advanced Threat Analytics  
Cloud App Security  
Intune  
Windows Server 2016  
SQL Server 2016



Windows Trust Boot  
Device Guard  
Credential Guard  
Microsoft Passport  
Windows Hello  
Windows Defender ATP  
Windows Update for Business  
Windows Data Protection



Azure Active Directory  
Azure Security Center  
Azure Storage Service Encryption  
Azure Key Vault  
Azure Information Protection



Advanced Threat Protection  
Anti-Spam / Anti-Malware  
Message Encryption  
Data Loss Prevention  
Threat Intelligence  
Advanced Data Governance  
Advanced eDiscovery  
Secure Score  
Customer Lockbox



© 2017 Microsoft Corporation. All rights reserved. The information herein is for informational purposes only and represents the current view of Microsoft Corporation as of the date of this presentation. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information provided after the date of this presentation. MICROSOFT MAKES NO WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS PRESENTATION.