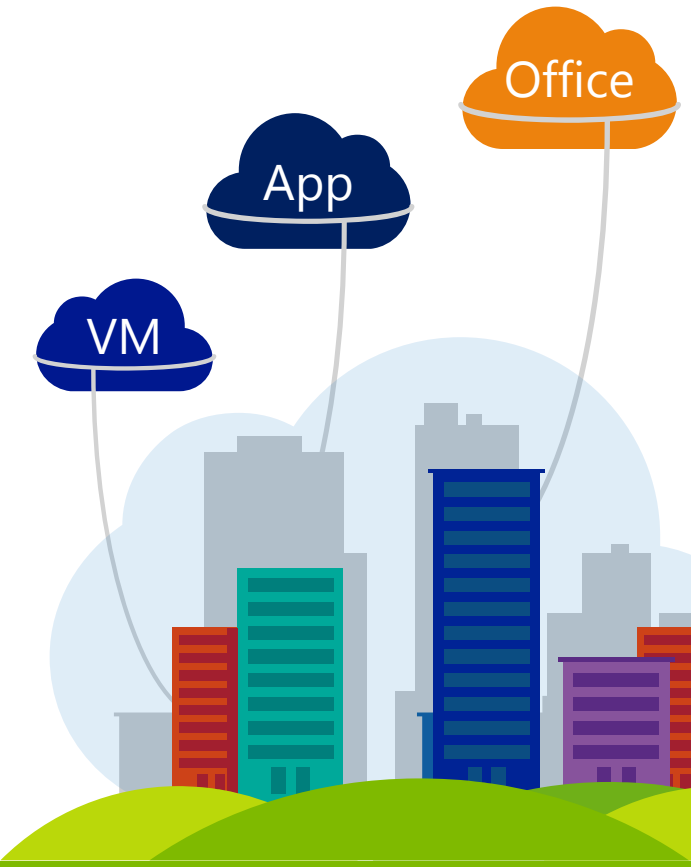
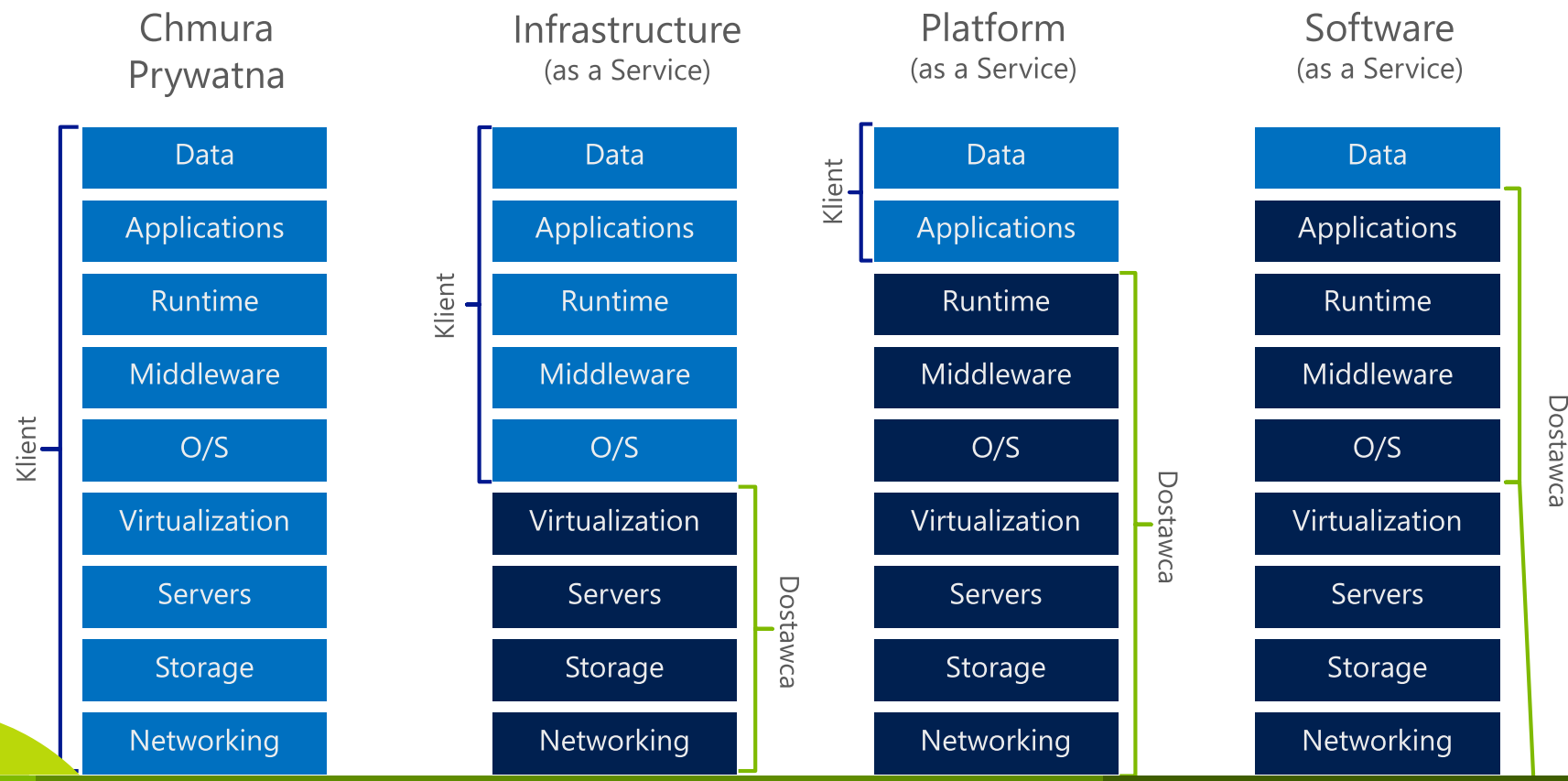
Nowy wymiar ochrony i zarządzania ryzykiem

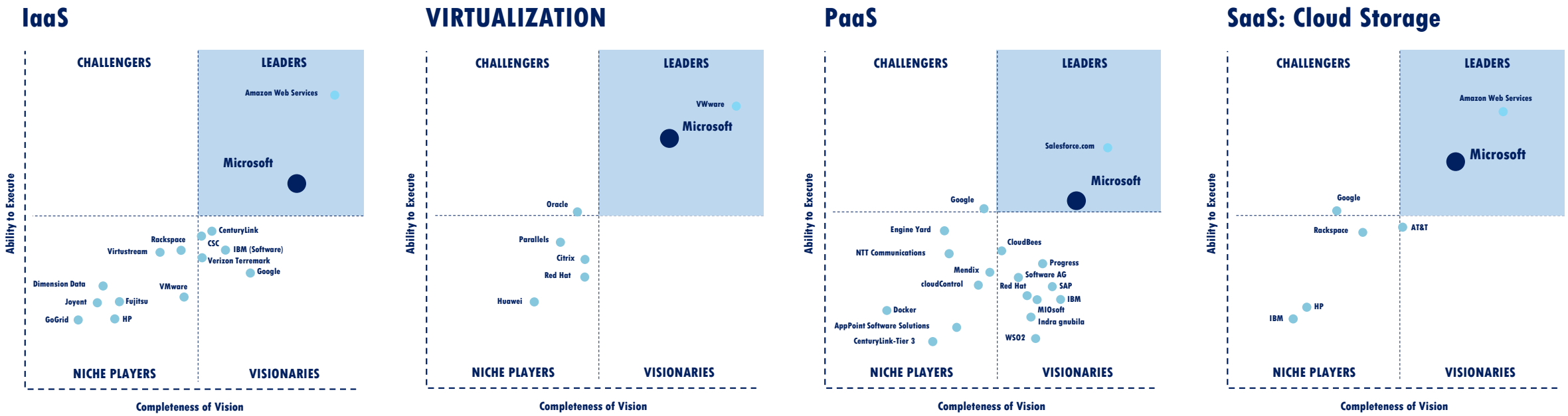
Marcin Nawrot – Cloud Solution Consultant – APN PROMISE
Maciej Sobianek – Cloud Platform Product Manager - MICROSOFT

Microsoft Cloud Platform





Microsoft Cloud Platform

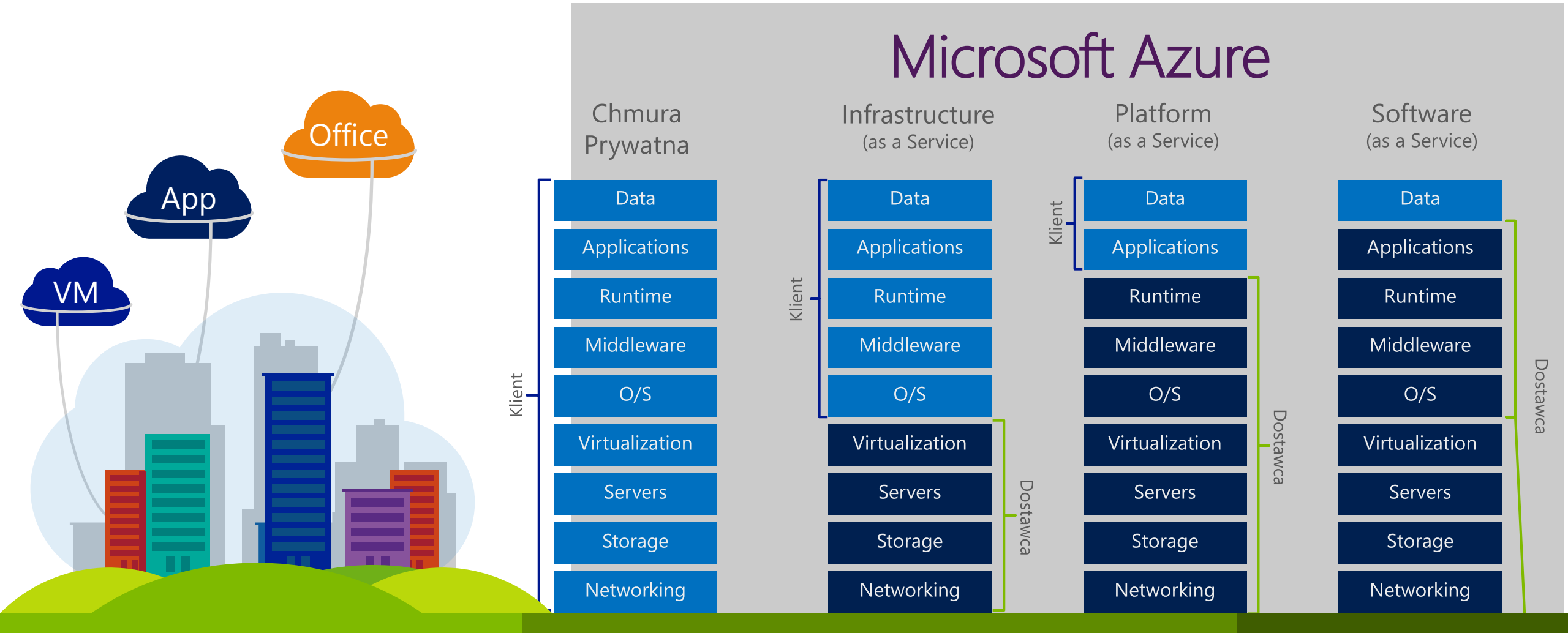


MICROSOFT DAJE NAM WYBÓR I ELASTYCZNOŚĆ

Źródło: Badania Gartner – Maj 2014

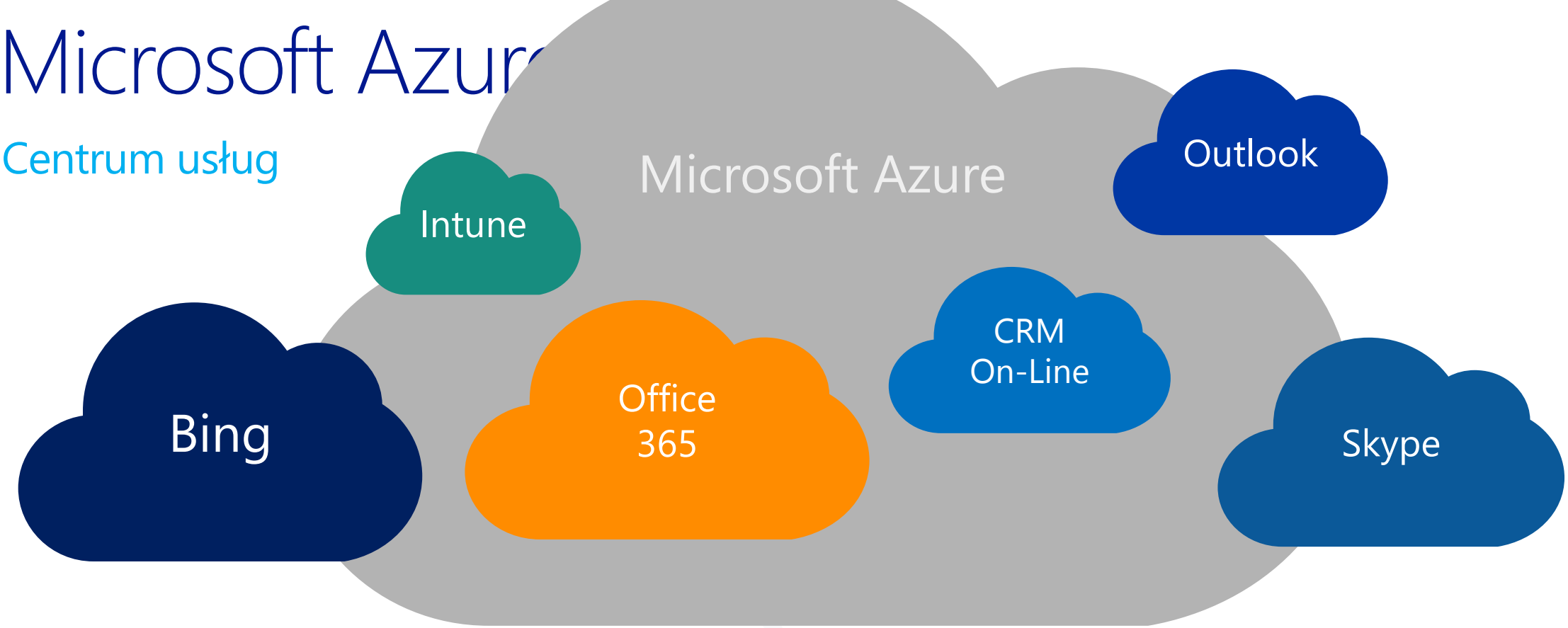
Microsoft Cloud Platform

Kompletny zestaw narzędzi do budowy hybrydowych rozwiązań IT.



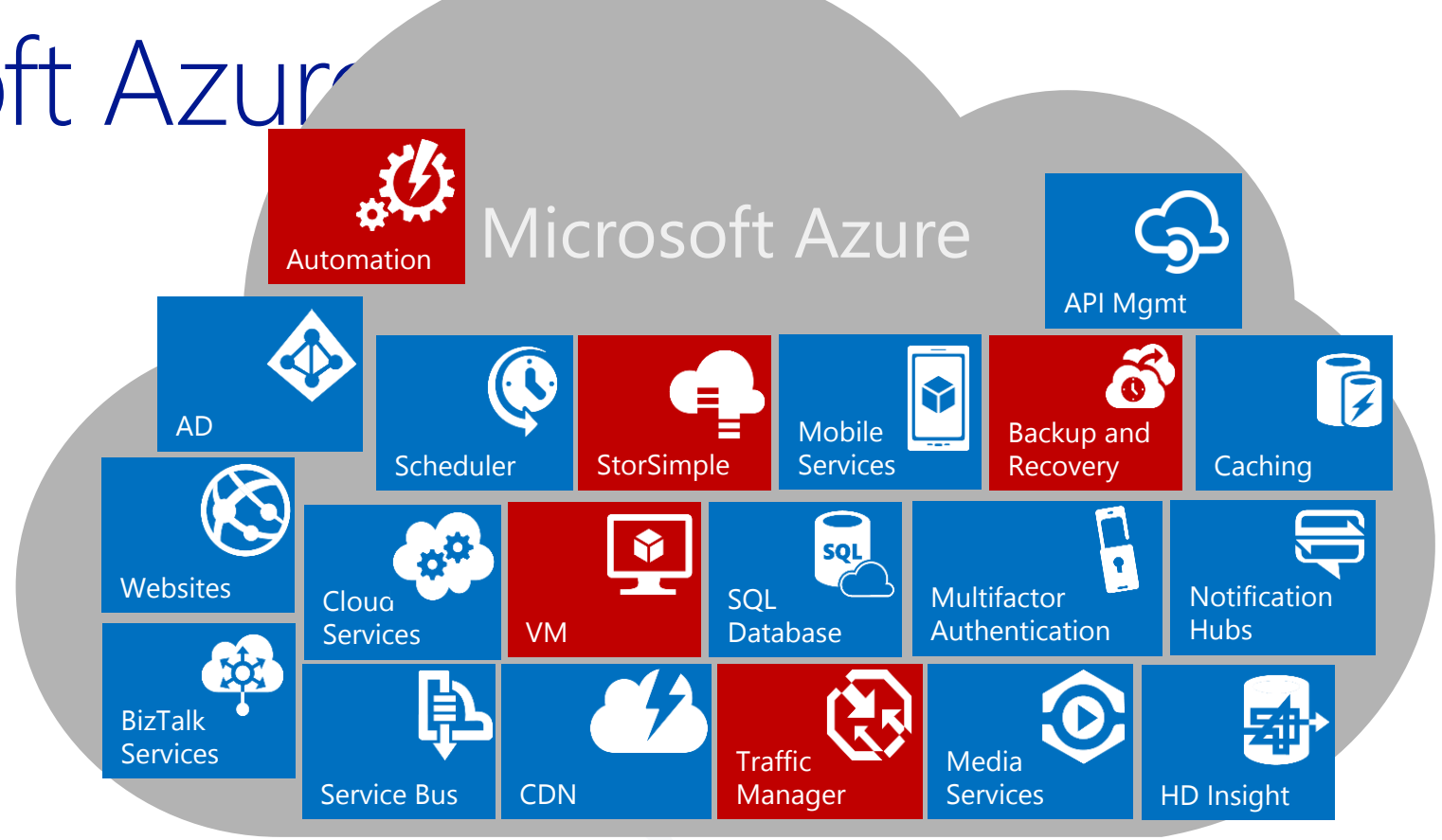
Microsoft Azur

Centrum usług



Microsoft Azur

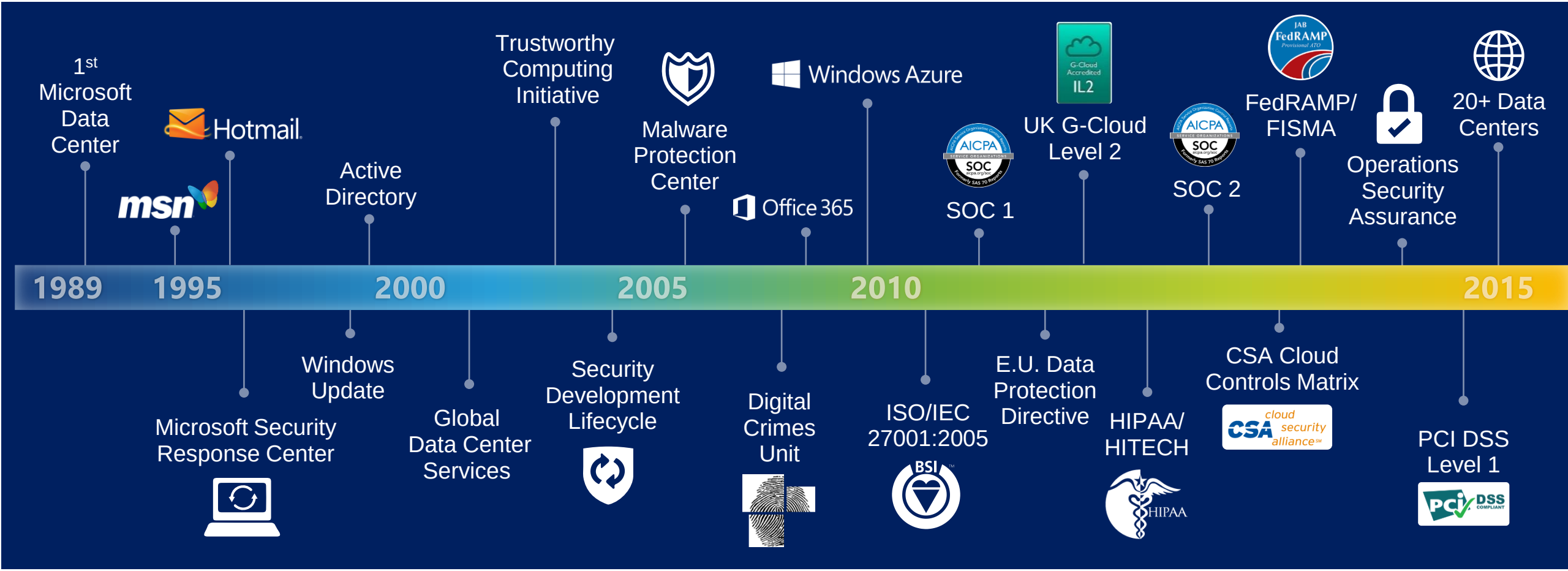
Centrum usług



100% ciągłości działania

Microsoft Cloud Platform

Od pierwszego Data Center do jednej z największych sieci usług



Podstawy zaufania do usług Microsoft

Dane są własnością KLIENTA

Klient nimi zarządza
Microsoft udostępnia narzędzia przetwarzania
Microsoft gwarantuje sposób ochrony i dostępność

Wbudowane zasady bezpieczeństwa

Ochrona danych jako podstawa usług

Stała zgodność ze zmieniającym się prawem i standardami

Transparentność wszystkich operacji

Niezależna weryfikacja

Lokalizacja danych i kontrola klientów nad nimi

Dlaczego powinno to interesować klientów?	• Zapewnienie przejrzystości co do miejsca posadowienia danych klientów jest ważne między innymi ze względu na konieczność wypełniania przepisów o ochronie danych osobowych • Wbrew rozpowszechnionemu błędnemu przekonaniu, zapewnienie konkretnego posadowienia danych klientów nie jest wystarczające by zapewnić im kontrolę nad ich danymi i zgodność z przepisami o ochronie danych osobowych • Kontrolę ze strony klientów oraz zgodność z przepisami o ochronie danych można zapewnić jedynie poprzez jednoznaczne zobowiązania umowne
Do czego zobowiązuje się Microsoft?	• Microsoft udostępnia publicznie w swoich Centrach Zaufania poszczególnych produktów aktualne rozlokowanie danych dla poszczególnych regionów, szczegółowo opisując, gdzie znajdują się dane i w jakich konkretnych okolicznościach mogą zostać przeniesione do innej lokalizacji (zapewnienie redundancji, prace konserwacyjne, itp.) • Microsoft oferuje środki umożliwiające klientom utrzymanie skutecznej kontrolii nad ich danymi (rozszerzone prawa administratorów, odwracalność, itp.)

EU Data Protection Authorities oceniło podejście Microsoft do ochrony prywatności

Article 29 Working Party – zespół „Inspektorów Ochrony Danych Osobowych" krajów UE

Ocena klauzul umownych przedstawionych przez Microsoft - EU Model Clauses. (Office 365, Azure, CRM Online, and Intune)

- Microsoft jest jedynym podmiotem, który otrzymał pozytywną opinię
- Od 1 czerwca klauzule umowne stanowią część umowy

Microsoft gains EU security approval

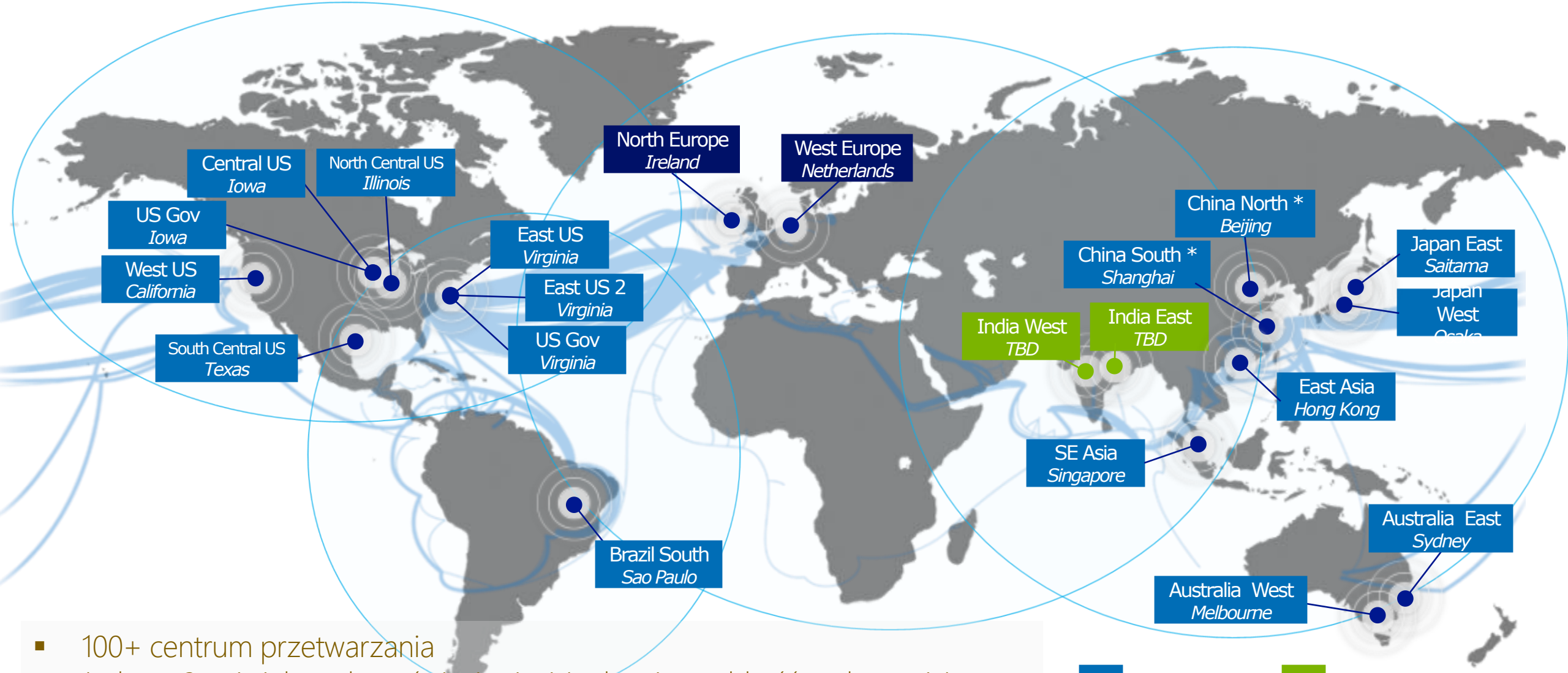
April 22, 2014 - 13:02 by Guy Wright

Tweet 0 | +1 0 | Share 0 | Submit | Share 0 | Share 4

Last week Microsoft announced that European Union's data protection authorities have found that Microsoft's enterprise cloud contracts meet EU privacy law standards. This is good news for companies using Microsoft's enterprise cloud services – in particular, Microsoft Azure, Office 365, Microsoft Dynamics CRM, and Windows Intune.

http://www.tgdaily.com/enterprise/100136-microsoft-gains-eu-security-approval

Microsoft Azure Datacenters



- 100+ centrum przetwarzania
- Jedna z 3 największych na świecie sieci (pokrycie, szybkość, połączenia)
- Liczba lokalizacji większa 2x od AWS oraz 6x od Google

Produkcyjne W budowie

* Obsługiwane przez 21Vianet

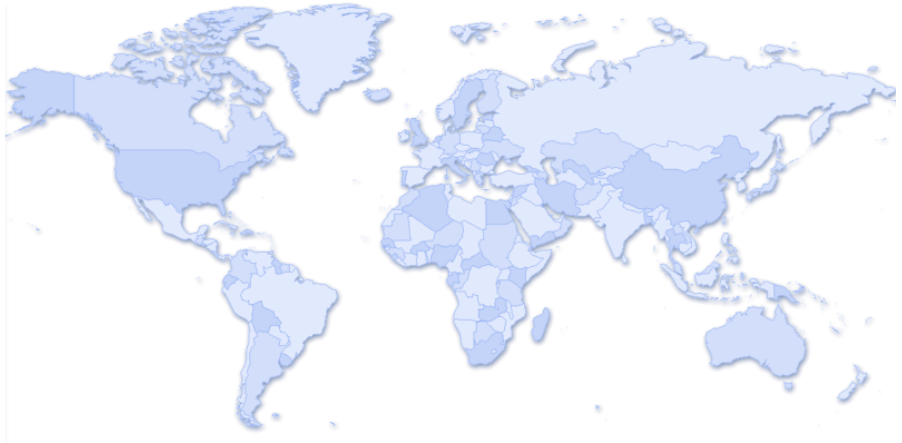
Wykorzystywanie danych klientów przez dostawcę chmury obliczeniowej

Dlaczego powinno to interesować klientów?	• Niektórzy dostawcy usług w chmurze skanują i wykorzystują dane klientów do swoich własnych celów komercyjnych (np. reklamowych) • Klienci powinni mieć pełną świadomość tego, oraz kontrolę nad tym, jak ich dane będą wykorzystywane przez dostawcę chmury obliczeniowej
Do czego zobowiązuje się Microsoft?	• Microsoft w swoich Umowach o Przetwarzaniu Danych zobowiązuje się do wykorzystywania danych klientów WYŁĄCZNIE w celu świadczenia usług tym klientom. • Microsoft nie rejestruje, nie zachowuje, nie skanuje, nie udostępnia ani nie wykorzystuje danych klientów w celach reklamowych.

Jasna sytuacja podwykonawcy

Dlaczego powinno to interesować klientów?	• Klientów powinno interesować, w jaki sposób ich dostawcy usług chmurowych korzystają z usług podwykonawców i jakie zobowiązania umowne są w tym zakresie oferowane • Brak jawności w kwestii podwykonawców nie tylko podważa zobowiązania podejmowane przez dostawców chmury, ale prowadzi także do problemów z przestrzeganiem prawa ochrony danych UE
Do czego zobowiązuje się Microsoft?	• Microsoft udostępnia swoim klientom (w Centrum Zaufania) aktualny wykaz swoich podwykonawców i wykonywanych przez każdego z nich funkcji. • Microsoft będzie powiadamiał klientów z co najmniej 14 dniowym wyprzedzeniem o dodawaniu nowych podwykonawców, a jeżeli klient nie akceptuje nowego podwykonawcy, ma prawo zakończyć używanie odnośnej Usługi Online. • Microsoft zobowiązuje swoich podwykonawców do zapewniania ochrony prywatności i poufności danych na poziomie zabezpieczeń co najmniej takim, do jakiego zobowiązuje się Microsoft w odniesieniu do danych klientów • Microsoft ponosi odpowiedzialność za swoich podwykonawców

Standardy i certyfikacje



Certyfikacje	Wertykał	Region
SSAE/SOC	Finance	Global
ISO27001	Global	Global
EUMC	Europe	Europe
FERPA	Education	U.S.
FISMA/FedRAMP	Government	U.S.
HIPAA	Healthcare	U.S.
HITECH	Healthcare	U.S.
ITAR	Defense	U.S.
HMG IL2	Government	UK
CJIS	Law Enforcement	U.S.
IRS 1075	Government	US
Article 29	Europe	Europe
SOC 2	Global	Global

Standardy w chmurze – dziś i jutro

- Dzisiaj używane standardy techniczne przy opisie cloud computing
  - ISO 27001 Information Security Management System
    Microsoft: http://www.microsoft.com/online/legal/v2/en-us/MOS_PTC_Security_Audit.htm

- Wprowadzane normy techniczne
  - ISO 17788 – definicje w cloud computing (vocabulary) – przyjęty 10.10.2014
  - ISO 17789 – architektura referencyjna cloud computing – przyjęty 10.10.2014
  - **ISO 27018** – normy dla *data processor* – przyjęty 27.07.2014
  - ISO 19086 – standardy SLA w cloud computing – Q4 2015/Q1 2016

Podstawowe zapisy ISO 27018

- ISO 27018 provides appropriate technical and organizational measures to protect personal data

- A personal data processor [*np. Microsoft*] and the personal data controller [*klient*] occupy distinct roles in the handling of personal data; the personal data processor supports the personal data controllers compliance with appropriate regulation.
- A successful third-party audit of a personal data processors support for ISO 27018 is a proof of conformance to the standard in support of the customer's regulatory obligations.
- „PII to be processed under a data processing contract should not be processed for any purpose independent of the instructions of the cloud service customer…PII processed under a data processing contract should not be used by the cloud PII processor for the purposes of marketing and advertising without express consent. Such consent should not be a condition of receiving the service."
- Other key 27018 requirements relating to personal data comprise
  - Notify the customer of legally binding law enforcement requests to disclose customer data, unless such a disclosure is otherwise prohibited
  - breach notification: notify the customer in the event of any unauthorized access to personal data or to processing equipment or facilities resulting in loss, disclosure or alteration of personal data
  - "Data deletion after portability": retention period of customer data once contract has terminated (180 days max for Microsoft)
  - geographic location of data: identify countries where data may be stored.

W zakresie zainteresowań rządów...

Nie umożliwiamy jednostkom rządowym bezpośredniego dostępu do danych

Nie wspomagamy rządów w przełamywaniu szyfrowania danych i transmisji.

Nie generujemy luk programowych (back doors) i umożliwiamy rządom weryfikację naszego kodu.

Kontrolki

View Control

AC-0154: Unsuccessful Logon Attempts - Enforcement

View Implementation Details

Global Data

Attribute
Domain
AF Family
AF Control Name
Activity Name
Engineering Descrip
Ownership
Facing
Threat To Control M
Is Deprecated
Description

View Control

AC-0155: Unsuccessful Logon Attempts - Actions

View Implementation Details

Global Data

Attribute	Value
Domain	Technical
AF Family	Access Control
AF Control Name	AC-0155
Activity Name	Unsuccessful Logon Attempts - Actions
Engineering Description	Automation [Selection: locks the account/node for an [Assignment: organization-defined time period]; according to [Assignment: organization-defined delay algorithm]] when the maximum number of unsu
Ownership	Cust; WL
Facing	OUTWARDS
Threat To Control Matrix Score	
Is Deprecated	false
Description	The information system automatically [Selection: locks the account/node for an [Assignment: organizat delays next login prompt according to [Assignment: organization-defined delay algorithm]] when the r

Niezależna weryfikacja

Dlaczego powinno to interesować klientów?	• Nawet najmocniejsze zobowiązania umowne nie są nic warte, jeżeli nie można ich poddać niezależnej weryfikacji • Wzorcowe klauzule umowne UE dają klientowi prawo audytowania podmiotu przetwarzającego jego dane poza EOG • Audytowanie usług online współużytkowanych przez wiele podmiotów (Mutli-Tenant Online Services) nie jest zadaniem łatwym i wielu klientów nie dysponuje czasem, personelem ani wiedzą techniczną niezbędną do ich przeprowadzania
Do czego zobowiązuje się Microsoft?	• Microsoft zobowiązuje się w umowie do audytowania swoich usług online pod kątem zgodności z normą ISO 27001 przez niezależny podmiot zewnętrzny (obecnie BSI) co najmniej raz w roku • Na pisemne żądanie klienta, Microsoft udostępni mu poufne streszczenie Sprawozdania z Kontroli Microsoft

Audytorzy

Audyty **ISO 27001** - BSI.

Audyty **ISAE3402/SOC** - Deloitte LLP.

Inne audyty – między innymi SecureInfo i Veris Group.

Raport audytu ISO – przykład

bsi.

Klienci mogą żądać kopii raportów audytowych

Prawo do analizy audytów

Management Summary.

Overall Conclusion

The objectives of this assessment have been achieved.

I would like to thank all the audit participants for their assistance and co-operation which enabled the audit to run smoothly and to schedule.

Based on the objective evidence detailed within this report, the areas assessed during the course of the visit were found to be effective.

Corrective actions with respect to nonconformities raised at the last assessment have been reviewed and found to be effectively implemented.

No new nonconformities were identified during the assessment. Enhanced detail relating to the overall assessment findings is contained within subsequent sections of the report.

Zarządzanie ryzykiem

Monitoring, zasady zgodności i audyty służą ograniczaniu ryzyka.

Ryzyko jest wpisane w działanie – należy je tylko MINIMALIZOWAĆ.

Jak zarządzać ryzykiem?
Ograniczać, przenosić, akceptować i unikać.

Microsoft Cloud Platform – Microsoft Azure

Wiele obszarów do dyskusji

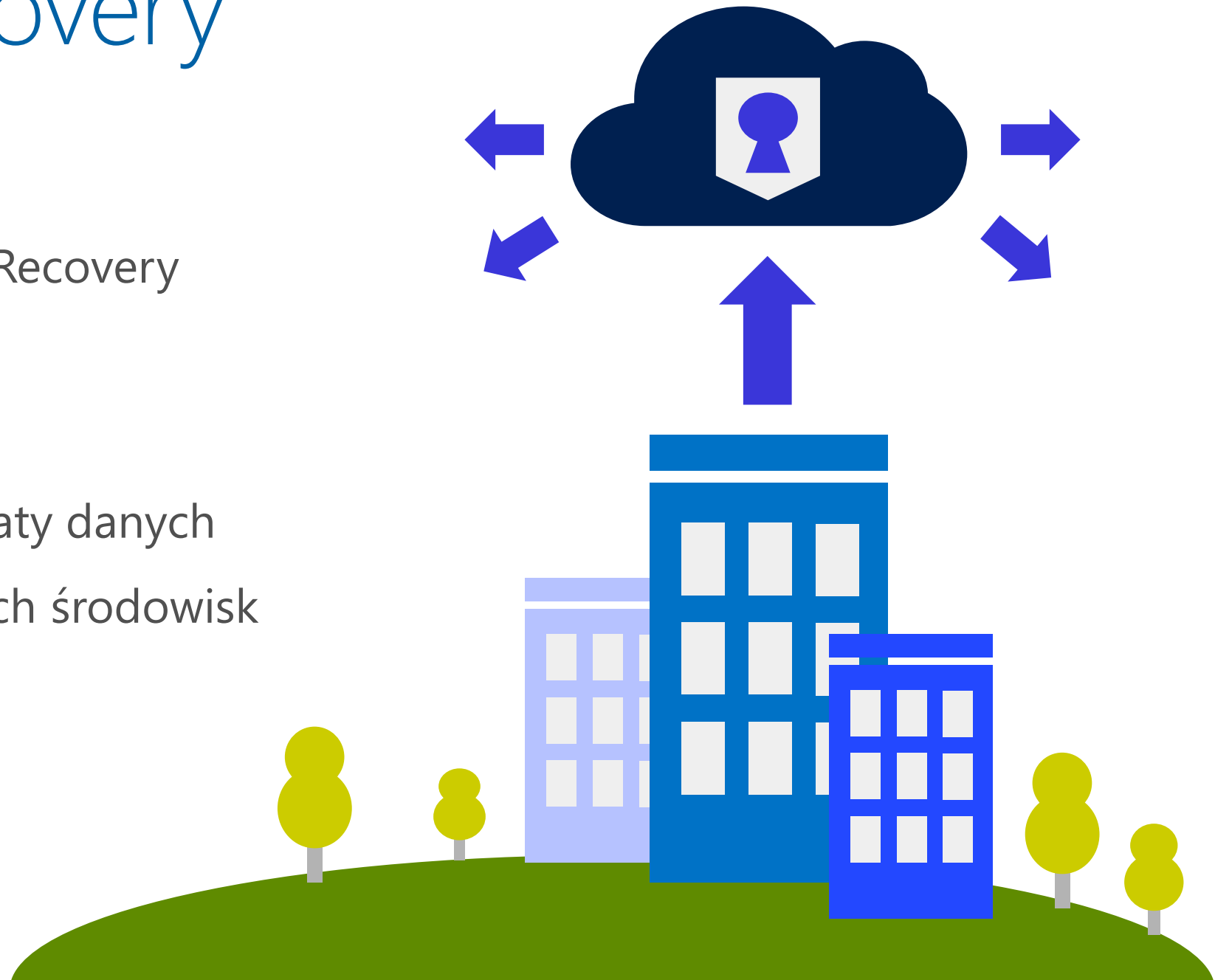
- Zgodność z dyrektywą **EU Data Protection Directive (95/46/EC)** oraz **Safe Harbor Framework** daje możliwość przechowywania i przetwarzania w chmurze Microsoft danych osobowych obywateli Unii Europejskiej w tym obywateli Rzeczpospolitej Polski.
- 28 inspektoratów ds. ochrony danych osobowych **(w tym polski Generalny Inspektor Ochrony Danych Osobowych)** zatwierdziło zobowiązania Microsoft w zakresie rozwiązań w chmurze.
- Centra przetwarzania danych Microsoft są poddawane **cyklicznym Audytom Bezpieczeństwa** realizowanym przez niezależne jednostki – Klienci mają pełny wgląd w raporty i analizy.
- Dane przed wysłaniem do chmury Microsoft mogą zostać zaszyfrowane kluczem x.509 v3 o długości 2048 bitów przed wysłaniem do chmury – Kluczem zarządza Klient i może przechowywać go poza chmurą Microsoft.
- Firma Microsoft gwarantuje **dostępność usług na poziomie 99,9% - 99,99%** Poszczególne wartości dostępności ustalane są indywidualnie dla danych komponentów platformy.
- **Infrastruktura Microsoft spełnia wymagania certyfikacyjne m.in. dla.:**
  - ISO/IEC 27001:2005 oraz SOC 1/SSAE 16/ISAE 3402 i SOC 2;
  - Cloud Security Alliance (CSA) oraz FedRAMP
  - Payment Card Industry (PCI) Data Security Standards (DSS)
  - UK G-Cloud, HIPAA BAA, Klauzuli modelowych UE, IRAP, MTCS,

Szczegółowe dane dotyczące dostępności, zgodności z przepisami prawa i międzynarodowymi certyfikacjami dostępne na stronie www w sekcji Trust Center.

Microsoft Azure Site Recovery

Azure Site Recovery

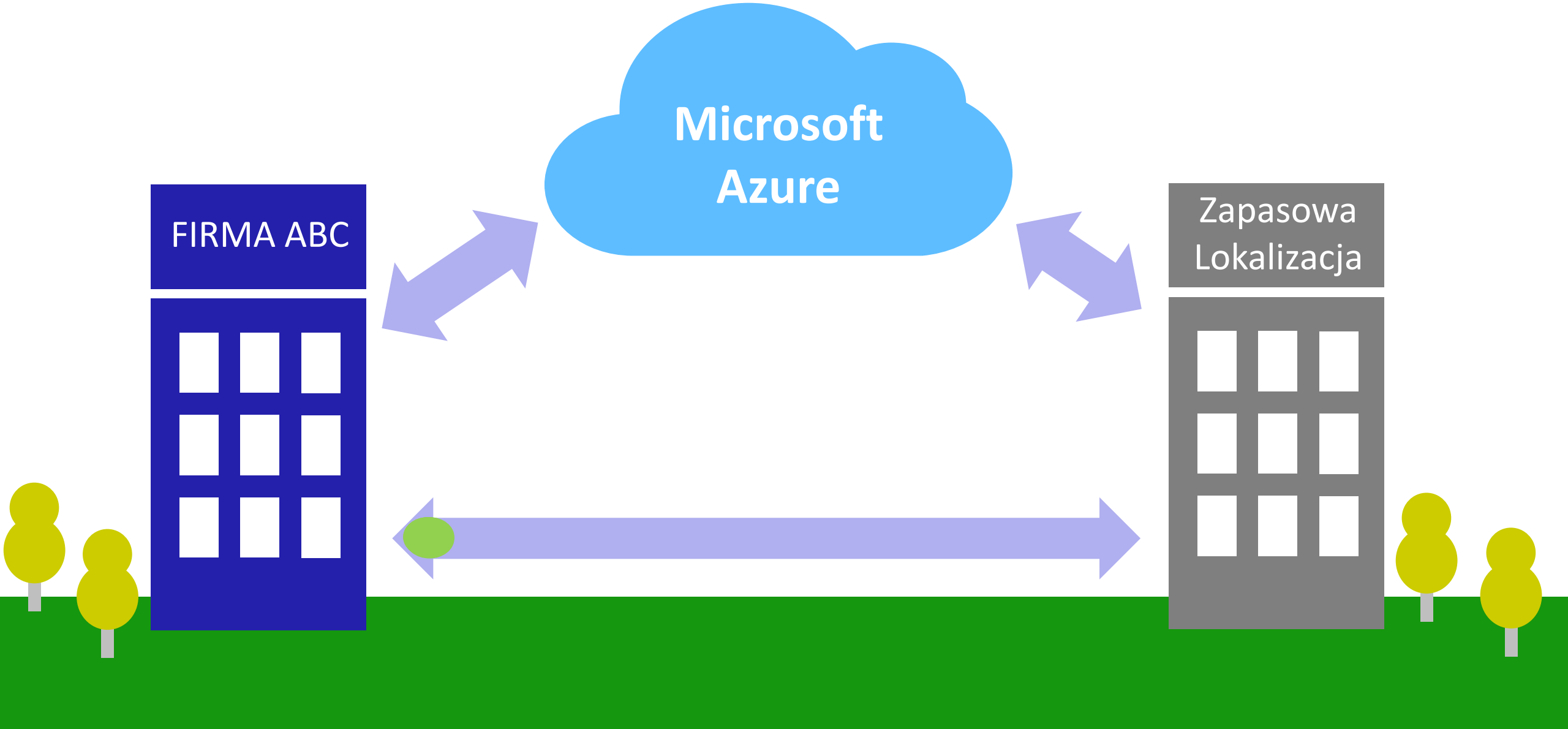
- Prosta procedura Disaster Recovery
- Ulepszone **RTO** i **RPO**
- Odizolowane testy
- Minimalizacja błędów i utraty danych
- Wspieranie niejednorodnych środowisk



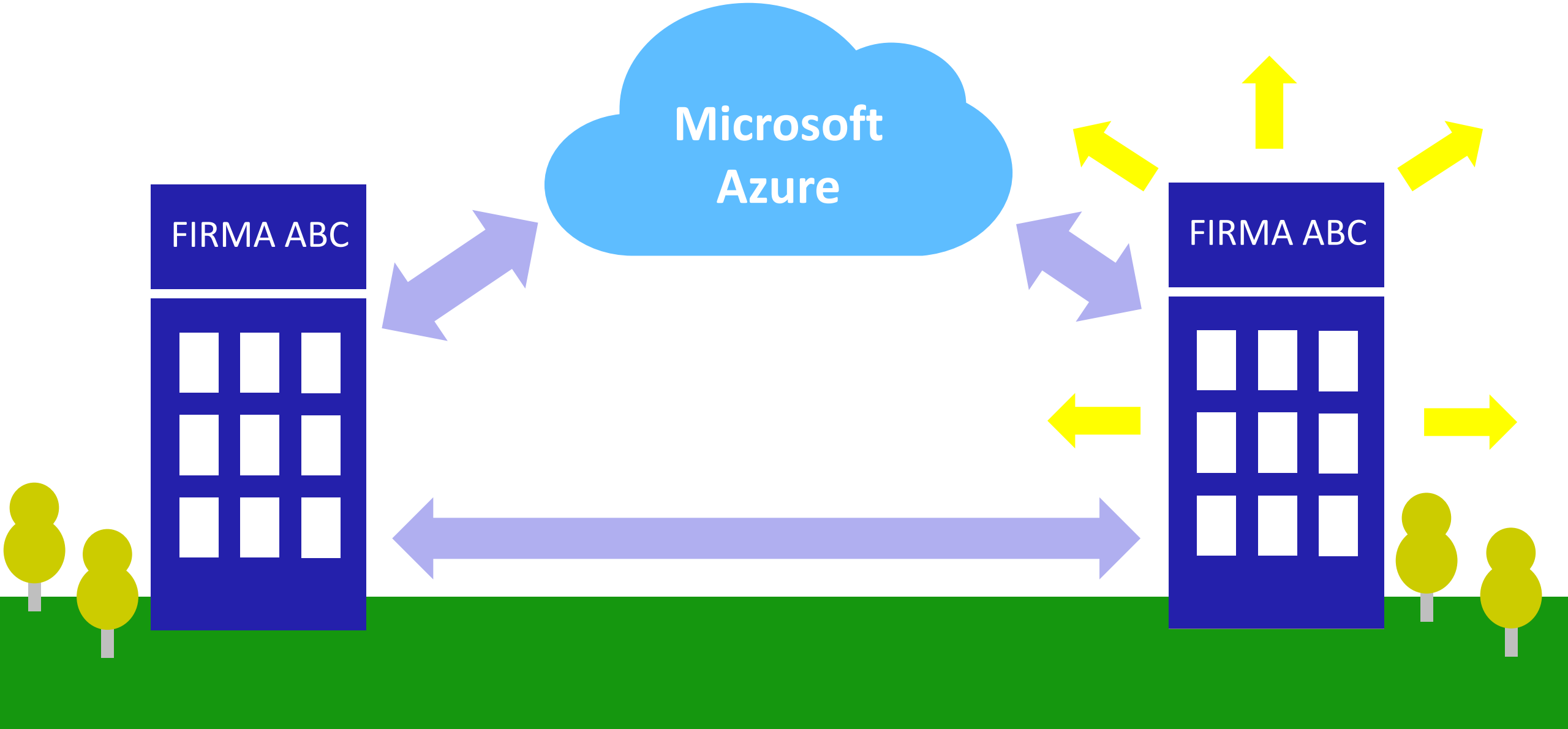
Jak to działa?

SCENARIUSZ 1

Firma ABC posiada zapasową lokalizację



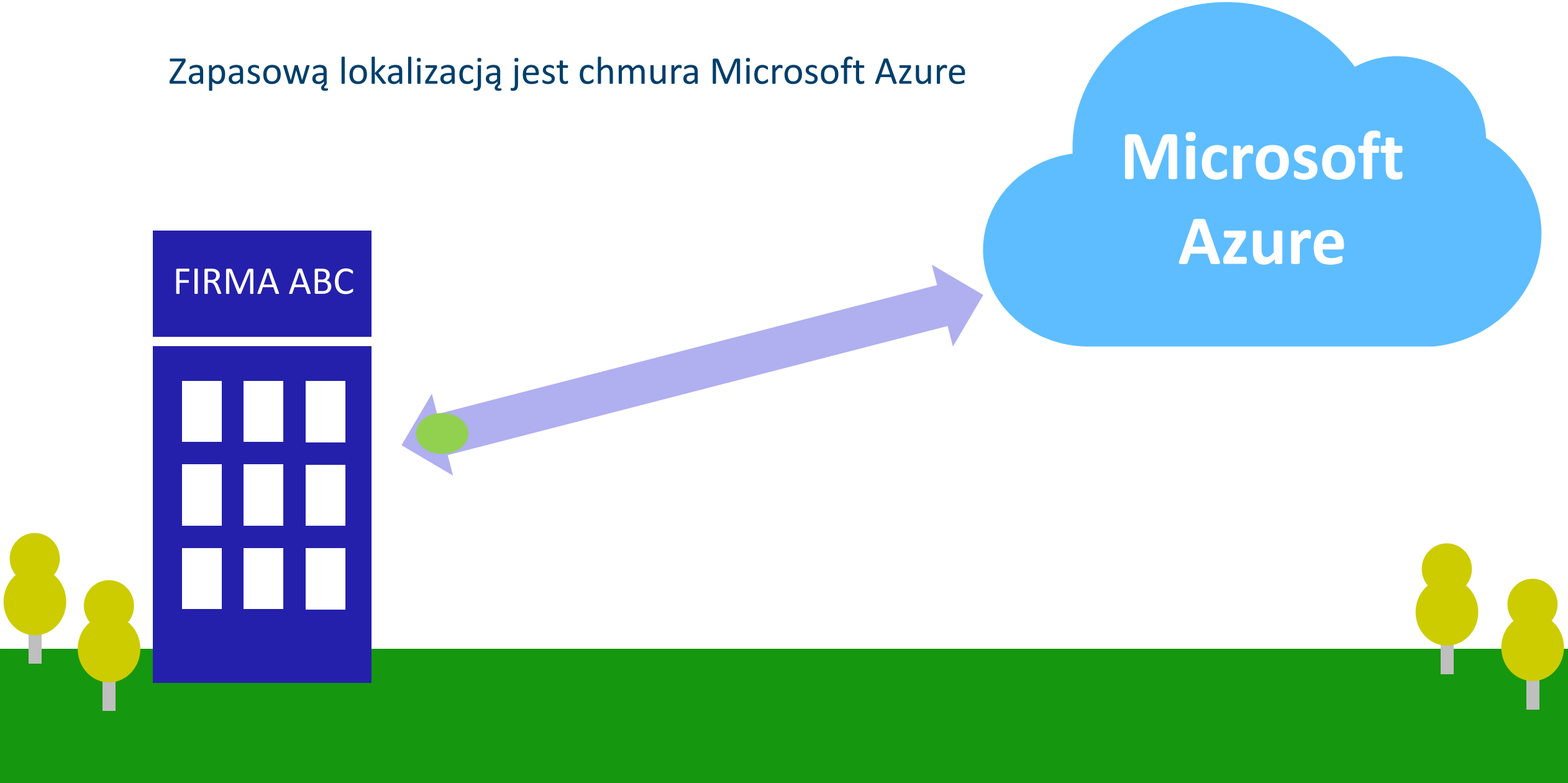
Firma ABC posiada zapasową lokalizację



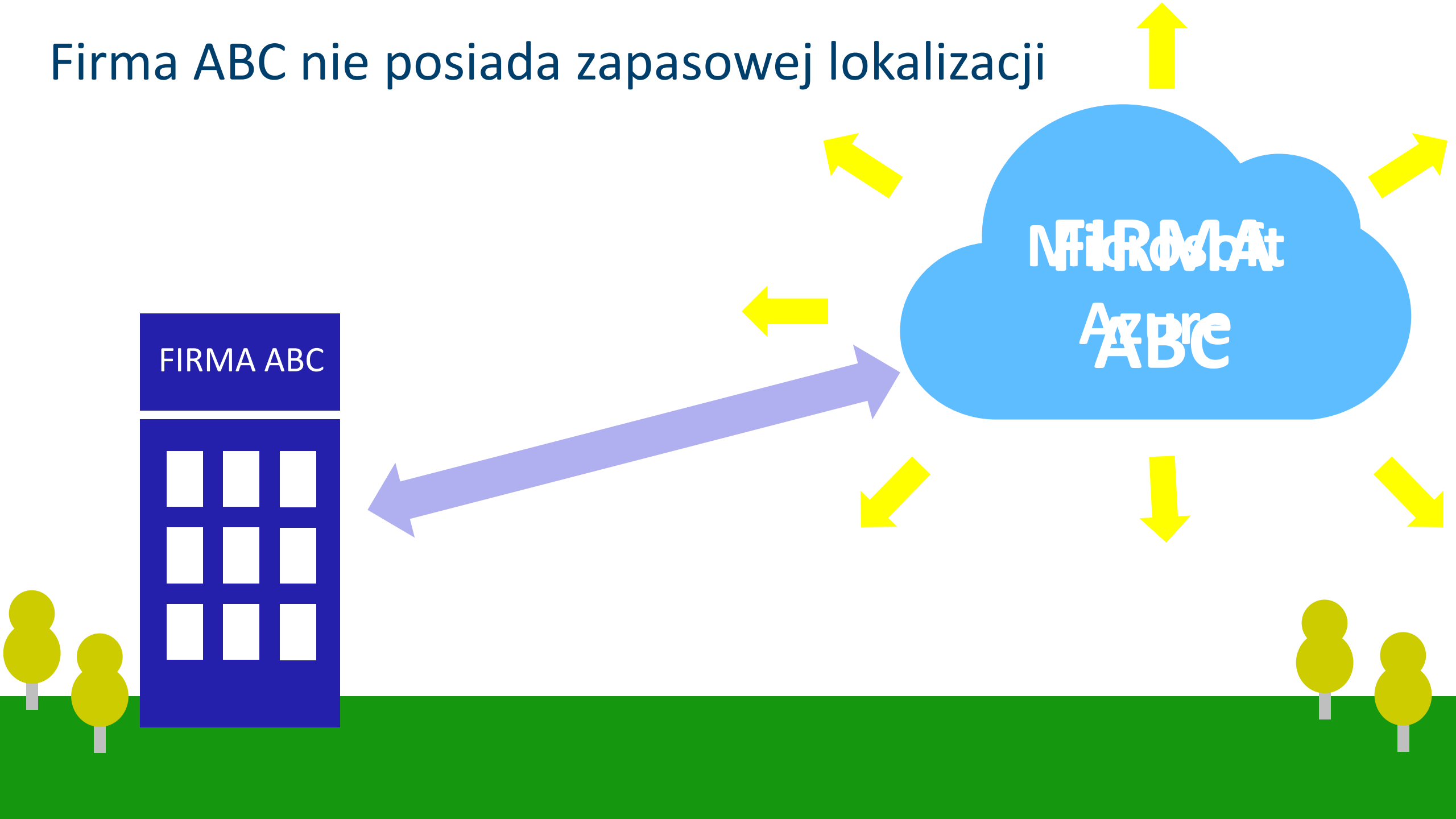
SCENARIUSZ 2

Firma ABC nie posiada zapasowej lokalizacji

Zapasową lokalizacją jest chmura Microsoft Azure



Firma ABC nie posiada zapasowej lokalizacji



Marcin Nawrot
marcin.nawrot@promise.pl

Maciej Sobianek
maciej.sobianek@microsoft.com