GDPR a ochrana osobních údajů

Michal Koščík

PrF MU; LF MU

Základní filosofie

Každý, kdo spravuje nebo zpracovává osobní údaje musí mít od počátku promyšleno k čemu tyto osobní data potřebuje a jak je bude chránit

„Data protection by design and by default“ Česky: „zásady záměrné a standardní ochrany osobních údajů“

Důraz na zachování integrity a důvěrnosti dat

Klade se velký důraz na samoregulaci uvnitř instituce

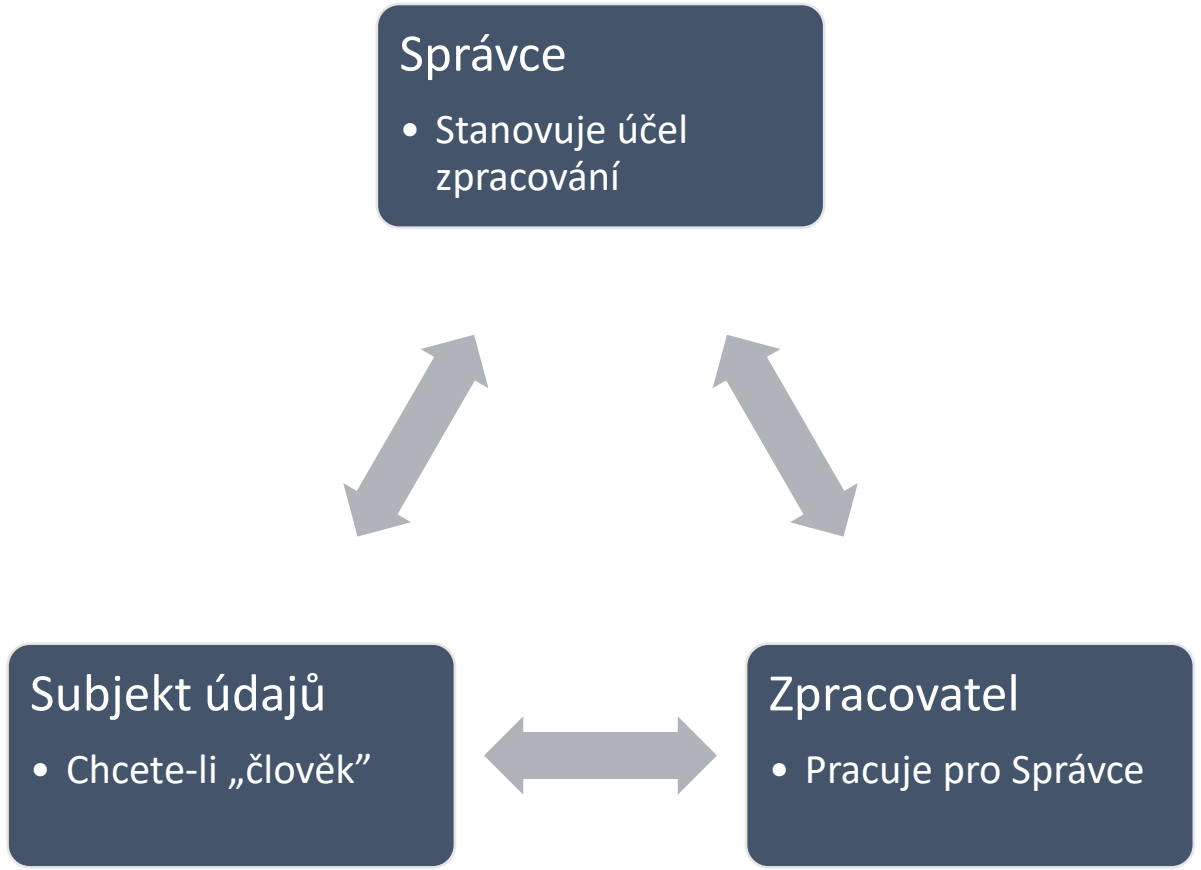
Největší problém – instituce musí vést záznam o tom, že tato pravidla dodržuje (protokol, data management plan etc.)

Výčet základních zásad

- zákonnost, korektnost, transparentnost
- účelové omezení
- minimalizace údajů (co do rozsahu)
- přesnost
- omezení uložení (časové)
- integrita a důvěrnost
- odpovědnost


ÚČEL
Účelové omezení
Nezpracovávat data k jinému účelu
Minimalizace dat
Rozsah sbíraných dat musí odpovídat účelu
Časové omezení
Data se musí po splnění účelu smazat nebo anonymizovat

Principy


Správce
• Stanovuje účel zpracování
Subjekt údajů
• Chcete-li „člověk”
Zpracovatel
• Pracuje pro Správce

Vztah správce a Zpracovatele

Správce rozhoduje o účelu informace	Zpracovatel
• Jedna informace může být ve správě vícero správců • Každý odpovídá sám za sebe	• Poskytovatel služby • Dělá pouze to co mu správce uloží • Pokud začne sám rozhodovat o účelu dat (informací) stává se správcem

Vztah správce - zpracovatel

Správce zpracováním pověřit pouze zpracovatele, kteří poskytují dostatečné záruky, zejména pokud jde o:

- odborné znalosti,
- spolehlivost a zdroje,
- technická a organizační opatření, která budou splňovat požadavky nařízení, včetně požadavků na bezpečnost zpracování.

Mezi správcem a zpracovatelem musí existovat **PÍSEMNÁ SMLOUVA**

TITUL k držbě a zpracování dat

Souhlas

- Může za správce získat i třetí subjekt
- Přísnější formální nároky (další slidy)

Zákonný důvod

- Pokud existuje zákonný důvod, lze sbírat bez souhlasu

Kdy je možné zpracovat data bez souhlasu?

- Plnění smlouvy
- Plnění právní povinnosti
- ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
- plnění úkolu prováděného ve veřejném zájmu
- při výkonu veřejné moci
- nezbytné pro účely oprávněných zájmů příslušného správce

Východiska souhlasu

- jednoznačným potvrzením, které je vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů, které se jej týkají,
- mlčení, předem zaškrtnutá políčka nebo nečinnost by tudíž neměly být považovány za souhlas. Souhlas by se měl vztahovat na veškeré činnosti zpracování prováděné pro stejný účel nebo stejné účely.
- lze předpokládat, že souhlas není svobodný, není-li možné vyjádřit samostatný souhlas s jednotlivými operacemi zpracování osobních údajů, i když je to v daném případě vhodné, nebo je-li plnění smlouvy, včetně poskytnutí služby učiněno závislým na souhlasu, i když to není pro toto plnění nezbytné.

Pravidla souhlasu (zkrácená)

- Správce musí být schopen doložit, že subjekt údajů udělil souhlas
- Pokud je souhlas subjektu údajů vyjádřen písemným prohlášením, které se týká rovněž jiných skutečností, musí žádost o vyjádření souhlasu předložena způsobem, který je od těchto jiných skutečností jasně odlišitelný, a je srozumitelný a snadno přístupný.
- Odvolat souhlas musí být stejně snadné jako jej poskytnout.
- Plnění smlouvy nesmí být podmíněno souhlasem se zpracováním.

Pravidla transparentnosti

Seznam informací, které musí být poskytnuty při získávání souhlasu (Čl. 13) a při zpracování (čl. 14)

Právo subjektu údajů na přístup k osobním údajům

- právo na informace o účelu a rozsahu
- právo na informace o zárukách
- Právo subjektu na opravu

Oznamovací povinnost ohledně opravy nebo výmazu osobních údajů nebo omezení zpracování (tam kde o to subjekt požádal Čl. 19)

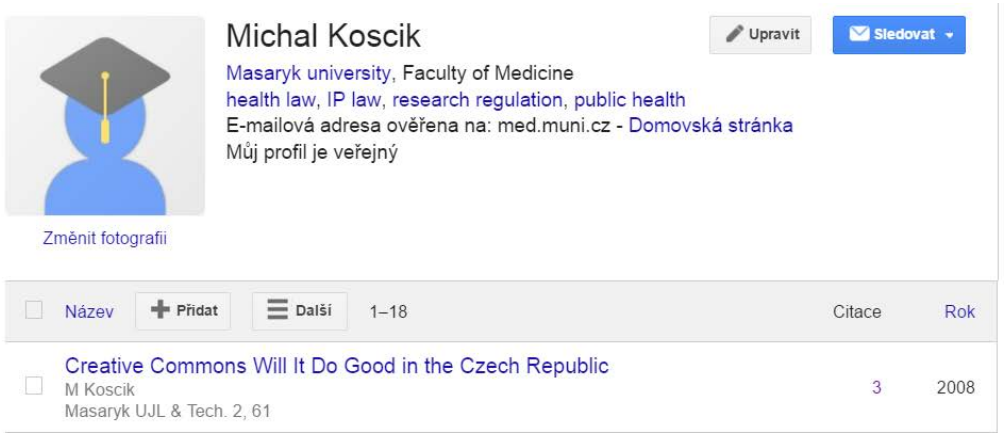
Právo na výmaz a omezení zpracování

Správce má povinnost osobní údaje vymazat, pokud subjekt údajů vznese námitky a neexistují žádné převažující oprávněné důvody pro zpracování

- výkon práva na svobodu projevu a informace
- splnění právní povinnosti
- z důvodů veřejného zájmu v oblasti veřejného zdraví
- pro účely archivace ve veřejném zájmu, pro účely vědeckého či historického výzkumu či pro statistické účely

Automatizované zpracování (profilování)

- Subjekt údajů má právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká.



Performativí pravidla a Kodexy chování

- Kodexy chování
  - Sdružení nebo jiné subjekty zastupující různé kategorie správců nebo zpracovatelů mohou vypracovávat kodexy chování nebo tyto kodexy upravovat či rozšiřovat, a to s cílem upřesnit uplatňování ustanovení tohoto nařízení
- Monitory
- Certifikáty
- Binding corporate rules – nadnárodní korporace

Doposud to nezní tak hrozně?

Nejobávanější část

Nejobávanější část

- **Záměrná a standardní ochrana osobních údajů (DP by design)**
- **Povinnost vést záznamy o činnostech zpracování**
- **Zabezpečení zpracování**
- **Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu**
- **Posouzení vlivu na ochranu osobních údajů**
- **Pověřenec pro ochranu osobních údajů**
- **Sankce**

Oblastí implementace GDPR

1. Interní legislativa
2. Registr zpracování OÚ
3. Metodiky
4. Posouzení dopadu
5. Úpravy systémů a procesů
6. Dokumentace
7. Vytvoření podpůrných systémů
8. Smluvní ujednání
9. Souhlasy SÚ
10. Pověřenec pro ochranu OÚ
11. Školení, informovanost

Data protection by design - Záměrná a standardní ochrana osobních údajů -

Starý koncept, nové definice, nové papíry

Odpovědnost za osobní údaje vzniká dříve než získáte první osobní údaje

Povinnost nastavit vnitřní procesy tak, aby nedocházelo k únikům a porušováním práv

Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné

Správce má povinnost vhodné úrovně bezpečnosti kdy zohlední zejména rizika, která představuje zpracování osobních údajů

Ochrana osobních údajů a softwarové databáze

Tři základní pohledy

Výrobce „krabicového“ software

- Jednoduchá situace
- Úplná kontrola nad obsahem

SaaS

- Nezbytná odpovědnosti za data uživatelů
- Odpovědnost dvojí – vůči uživatelům i vůči třetím stranám

Agregátoři, Chatboti, Učící se programy

- Cílem programu je se nezávisle rozšiřovat o data

Recommended

Office 365 Home

5 PCs or Macs plus 5 iPads or Windows tablets.[1]

- 20GB each for up to 5 users[3,6]
- 60 minutes of Skype calls per month[4]
- Ongoing access to updates

$99.99 1-year subscription

Suite includes:

Word, Publisher[2], Excel, Access[2], PowerPoint, OneDrive, OneNote, Skype[2], Outlook

New

Office 365 Personal

For 1 PC or Mac plus 1 iPad or Windows Tablet. [1]

- 20GB each for up to 1 user[3,6]
- 60 minutes of Skype calls per month[4]
- Ongoing access to updates

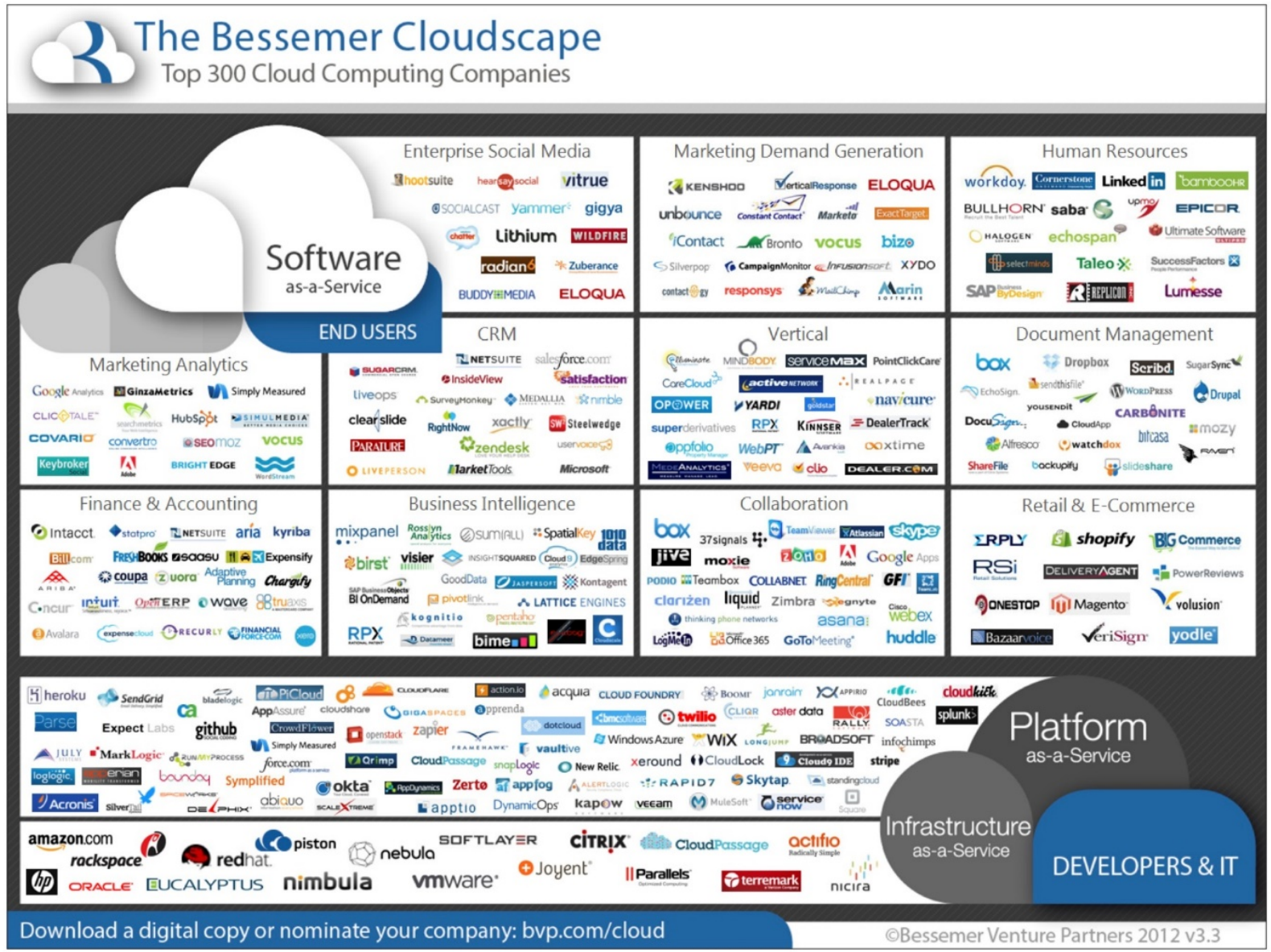
$69.99 1-year subscription

Suite includes:

Word, Publisher[2], Excel, Access[2], PowerPoint, OneDrive, OneNote, Skype[2], Outlook

The Bessemer Cloudscape

Top 300 Cloud Computing Companies



Download a digital copy or nominate your company: bvp.com/cloud

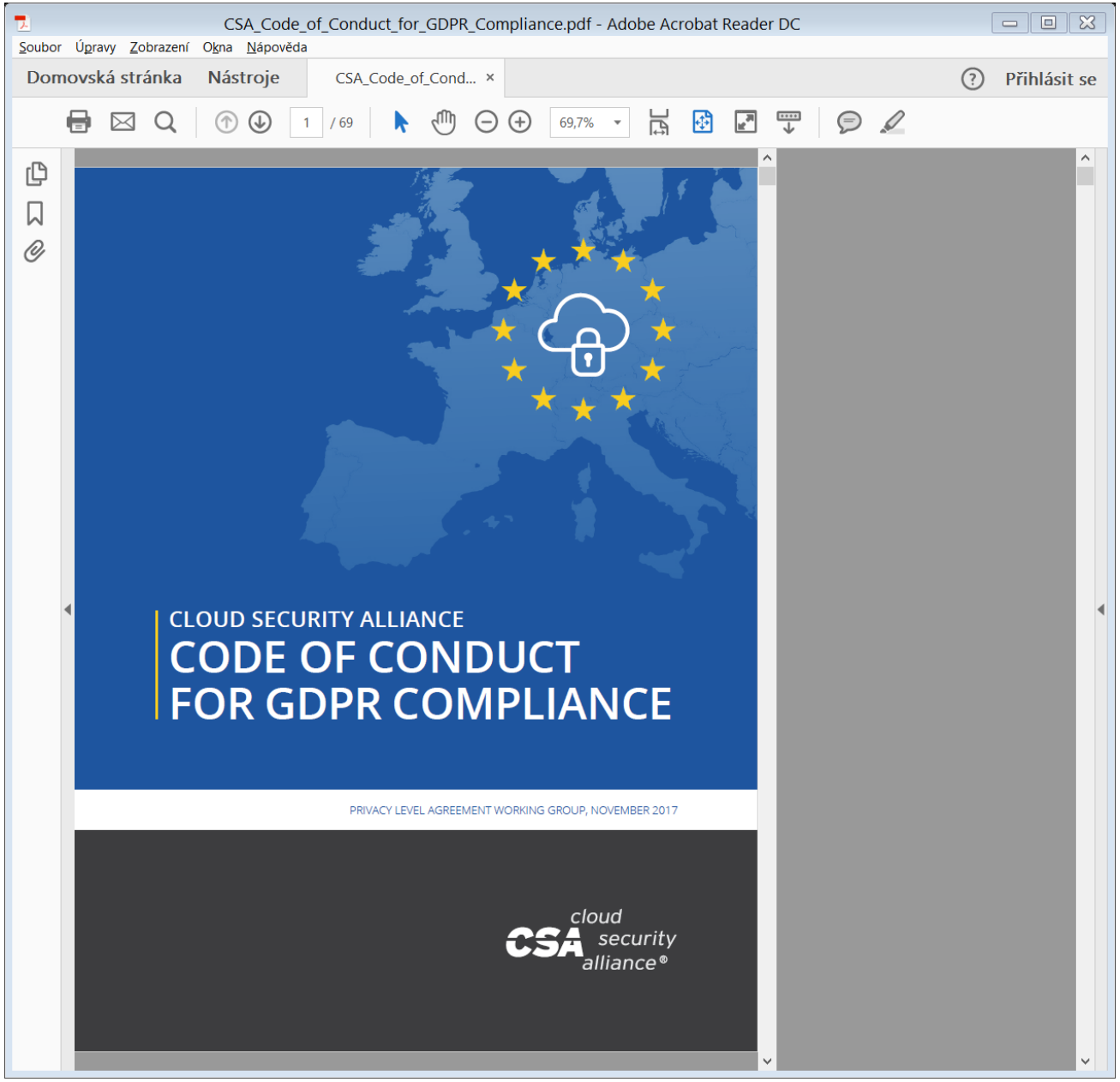
Ochrana dat

- Bezpečnost dat
  - Před ztrátou
  - Před zveřejněním či únikem
- Ochrana osobních údajů uživatele
  - Poskytovatel cloudové „síťové“ služby je často správcem i zpracovatelem


EU Data Protection
Code of Conduct for Cloud Service Providers
v. 1.7
May 2017
EU
CLOUD
COC

Článek 40 GDPR

- Odst. 1. - Členské státy, dozorové úřady, sbor a Komise podporují vypracování kodexů chování, které mají přispět k řádnému uplatňování tohoto nařízení s ohledem na konkrétní povahu různých odvětví provádějících zpracování a na konkrétní potřeby mikropodniků a malých a středních podniků


CSA_Code_of_Conduct_for_GDPR_Compliance.pdf - Adobe Acrobat Reader DC
Soubor Úpravy Zobrazení Okna Nápověda
Domovská stránka Nástroje
CSA_Code_of_Cond...
Přihlásit se
1 / 69
69,7%
CLOUD SECURITY ALLIANCE
CODE OF CONDUCT
FOR GDPR COMPLIANCE
PRIVACY LEVEL AGREEMENT WORKING GROUP, NOVEMBER 2017
cloud security alliance®

Části:

PART 1: CSA COC OBJECTIVES, SCOPE, METHODOLOGY,

PART 2: PRIVACY LEVEL AGREEMENT

PART 3: GOVERNANCE AND ADHERENCE MECHANISMS

- TECHNICAL COMPONENTS
- GOVERNANCE BODIES, ROLES AND RESPONSIBILITIES
- GOVERNANCE PROCESS AND RELATED ACTIVITIES

Předávání osobních údajů do zahraničí

- Adekvátní úroveň ochrany třetí země
- Posoudí komise
  - Kterákoliv země se může stát kdykoliv nedůvěryhodnou
  - Dopady do data management plánů

Citace obrázků

- Gymnastic students in a pyramid display, St. Petersburg, Russian Photographer, (20th century) / Private Collection http://www.bridgemanimages.com/en-US/explore/news/features/2014/April/hermitage
- *Detail of design for the Royal School of Mines (Imperial College of Science and Technology), perspective from the north east, 1910 Pen on paper Artist: Thomas Raffles Davison (1853-1937) Architect: Sir Aston Webb (1849-1930) Copyright: RIBA Library Drawings & Archives Collections http://preview2-riba.contensis.com/001Oldfolders/LibraryDrawingsAndPhotographs/Albertopolis/TheStoryOf/ImperialCollege/RoyalSchoolOfMines.aspx*
- *By Oscar Franzén (Own work) [Public domain], via Wikimedia Commons http://commons.wikimedia.org/wiki/File:KTH_Borgg%C3%A5rden_22072006.jpg*