Základní východiska GDPR

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

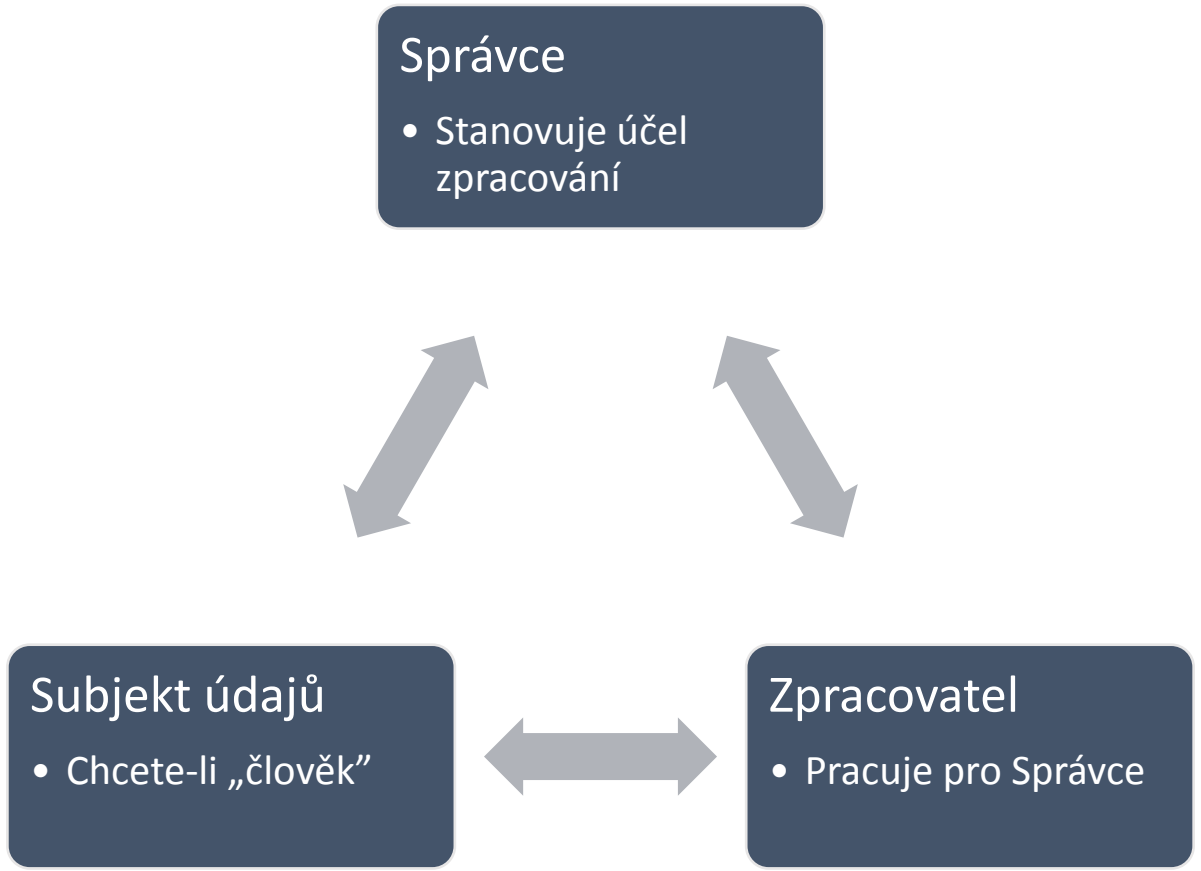
Největší problém – instituce musí vést záznam o tom, že tato pravidla dodržuje (protokol, data management plan etc.)

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)

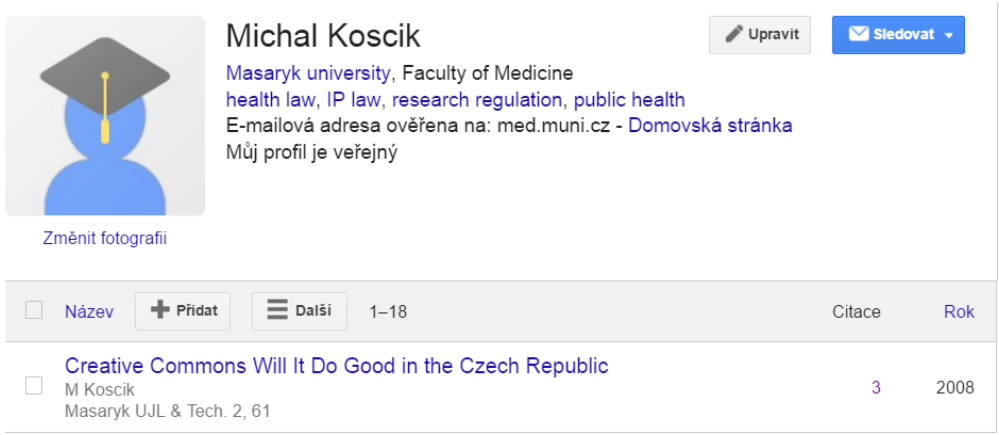
Právo na výmaz a omezení zpracování

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

1. Interní legislativa

- Institucionální směrnice – základ celé GDPR „stavby“
  - Základní pravidla
  - Struktury
  - Zodpovědnosti

- Spíš stručná, jen základní věci
  - Musí vyhovět i velmi heterogennímu prostředí
  - Detaily budou rozpracovány v metodikách

2. Registr zpracování OÚ

- Přehled o všech zpracováních OÚ v organizaci
  - Povinná část dle GDPR
  - Problém: granularita/identifikace jednotl. zpracování a jejich počet
- Průběžná aktualizace
- Implementace
  - Struktura záznamu, datový model
  - SW implementace – varianty
    - Modul integrovaný v interním univerzitním systému
    - Samostatný systém – opravený open-source
    - Společná služba pro více zájemců

3. Metodiky

- Návody a postupy v různých oblastech pro
  - Správce/administrátory systémů
  - Koncové uživatele
- Oblasti
  - Weby
  - Elektronická komunikace (e-mail, …)
  - Úložiště dokumentů (vlastní x externí – MS-O365,…)
  - Tvorba a provoz inf-systémů
  - Vybrané typy zpracování OÚ (dohledové systémy, …)
  - Mobilní zařízení (notebooky, …)
  - Vypořádání práv/požadavků SÚ, postupy při úniku OÚ, …

4. Posouzení dopadu

- 2úrovňové posouzení všech případů zpracování OÚ
  - Zjednodušené – u zpracování s nízkým rizikem
  - Plnohodnotné DPIA – u vysokého rizika
- Závěry a doporučení pro implementaci
- Metodiky a vzorová DPIA
  - projekt FR CESNET, Microsoft, …
- K ujasnění
  - Kdo bude jednotlivá posouzení provádět (správci inf-systémů?)
  - Kdo jim bude dávat „razítko“ že jsou OK (pověřenec?)

5. Úpravy systémů a procesů

- Implementace doporučení z posouzení dopadu
  - Organizační x technická
  - Pro každý systém mohou být jiná (šitá na míru)

- Nová věc: vypořádání s (novými) právy SÚ
  - Právo být zapomenut
  - Právo na informace
  - Právo na omezené zpracování
  - Právo na přenositelnost OÚ
  - …

6. Dokumentace, dokumentace

Dokumentace jako základ pro prokázání compliance

- Přehled všech zpracování (viz registr)
- Záznamy posouzení všech zpracování
- Případy porušení ochrany OU
- Souhlasy SÚ
- Závazky mlčenlivosti (správci, admini)
- Provedená školení
- …

7. Podpůrné systémy

- Registr zpracování
- Evidence souhlasů
- Dokumentační systém
- …

- Podpůrné externí systémy
- Vazba na systémy kybernetické ochrany

8. Souhlasy SÚ

- Zmapování současného stavu na univerzitě
  - Velmi různorodá praxe (případ od případu)
- Metodika dle GDPR – kdy, jak
  - Vazba na účely zpracování
  - Vzorové souhlasy
- Podpora, evidence
  - Centrální x lokální (ne vše půjde centralizovat)
  - Papírová x elektronická (ne vše je/bude on-line)

9. Pověřenec pro ochranu OÚ

- Pro MU (a další velké VŠ) nezbytný!
  - Sdílený pověřenec pro malé VVŠ?
- Požadavky na odbornost - vágní
- Začlenění v rámci organizace – nezávislost
  - Pověřenec není manažer, ale „malý úřad“
- Spolupráce pověřenců v rámci vysokých škol (?)

10. Smluvní ujednání

- Podchycení a revize smluv v působnosti GDPR
- Se zpracovateli dat pro univerzitu
  - Poskytovatelé cloudových služeb (MS-O365)
  - ISIC/ITIC (GTS), …
- Se správci dat, pro něž je univerzita zpracovatelem
  - Vymezení zpracovatele (viz Registr studentů VŠ, aj.)
- Doporučení, best-practices

11. Školení, informovanost

- Na různých úrovních
  - Vedení univerzity a jednotlivých součástí
  - Správci a administrátoři systémů
  - Koncoví uživatelé
  - Noví zaměstnanci
- Různou formou
  - Fyzická školení, prezentace
  - E-learning
    - Varianta samoproškolení zaměstnanců s e-potvrzením

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

Anonymizace, pseudonymizace a profilování

Anonymizované OÚ

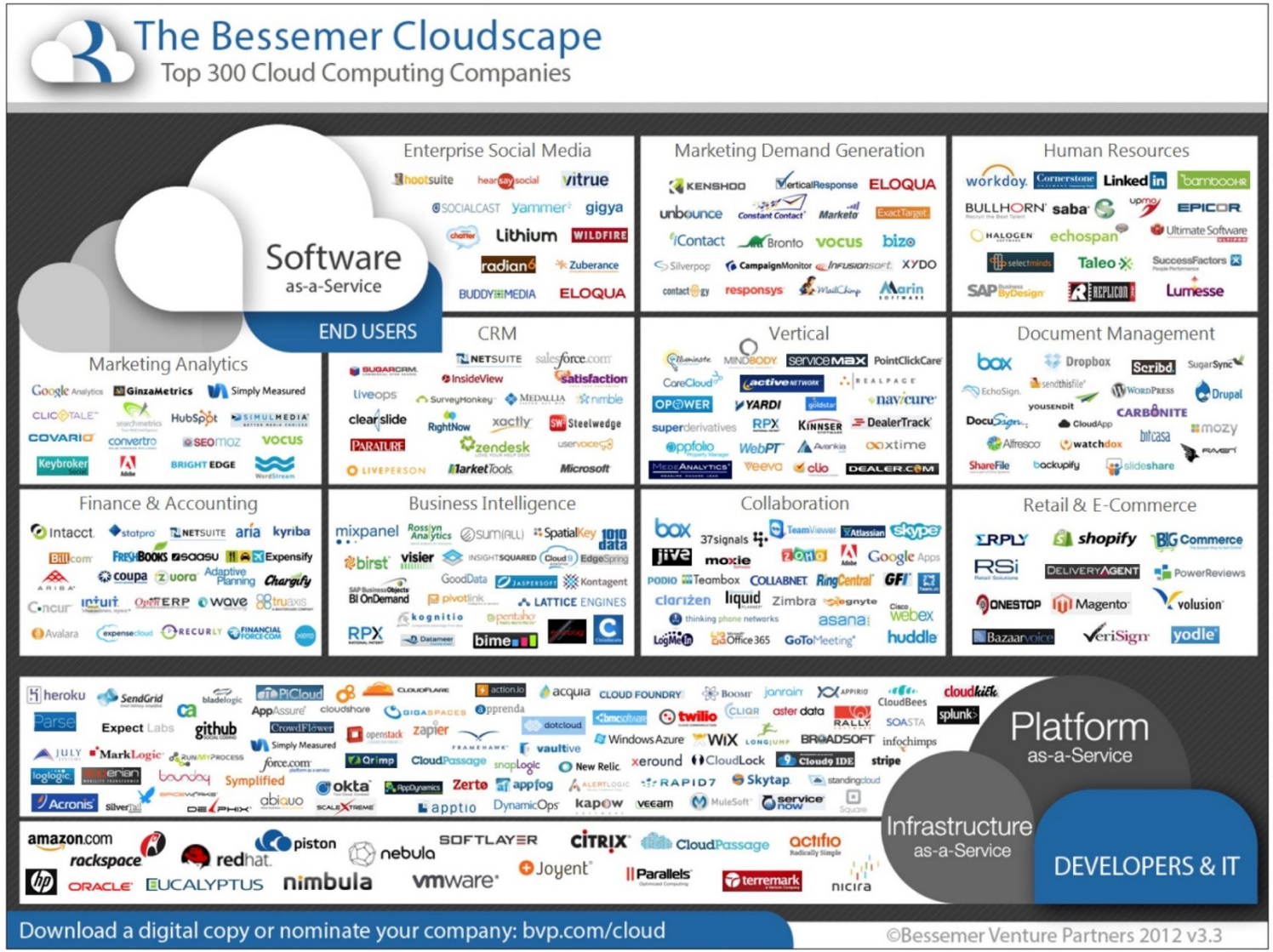
- Nelze dešifrovat, klíč je zničen

Pseudonymizované OÚ

- Lze dešifrovat, třeba za cenu velkého úsilí
- I tato data jsou OÚ

Profilování

- automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě


The Bessemer Cloudscape
Top 300 Cloud Computing Companies
Software
as-a-Service
END USERS
Enterprise Social Media
Marketing Demand Generation
Human Resources
Marketing Analytics
CRM
Vertical
Document Management
Finance & Accounting
Business Intelligence
Collaboration
Retail & E-Commerce
Platform
as-a-Service
Infrastructure
as-a-Service
DEVELOPERS & IT
Download a digital copy or nominate your company: bvp.com/cloud
©Bessemer Venture Partners 2012 v3.3

Ochrana dat

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