ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

GDPR
a rizika ochrany osobních údajů jinak

Miroslav Bartošek

Masarykova univerzita – Ústav výpočetní techniky

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

O čem to bude

1. Něco málo o GDPR
2. Proč jsme do toho šli
3. Komplexní systém ochrany na VŠ
4. Rizika – ale která a jak?
5. Příklad: Fotografie v organizaci
6. Mezi mlýnskými kameny
   – má zdravý rozum šanci?

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

1.1 General Data Protection Regulation

- Evropské nařízení o ochraně osobních údajů (č. 2016/679)
  - Přijaté 27. 4. 2016, účinné od **25. 5. 2018**
  - Nahrazuje směrnici 95/46/EC a národní úpravy států EU
- Nařízení → přímá účinnost v právním řádu všech zemí EU
  - Možnost upřesnění na národní úrovni (ÚOOÚ)
  - V ČR dosud Zákon č. 101/2000 Sb., o ochraně osobních údajů
    - Návrh nového zákona (oproti GDPR nic zásadního)
- Obsáhlá norma
  - 88 stran, 99 článků, 173 recitálů
  - Technologicky neutrální (co se má udělat, ale ne jak)

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

1.2 Co přináší GDPR nového

- Je to evoluce, nikoliv revoluce
  (**ale** velmi záleží na tom, jak byla ochrana OÚ nastavena v organizaci dosud)
- Zrušena registrační povinnost
  (**ale** nahrazena povinností dokumentační – změna paradigmatu)
- Posílena práva subjektů údajů
  (právo na informovanost, namítat, omezené zprac, být zapomenut, přenositelnost)
- Rozšířeny povinnosti správců/zpracovatelů dat
  (přístup založený na riziku)
- Drakonické sankce
  (až 20 mil EUR)

1.3 Hlavní zásady při zpracování OÚ

- Účel – a omezení dat vzhledem k účelu
- Zákonnost
- Transparentnost a korektnost
- Minimalizace údajů
- Časově omezené uložení
- Přesnost a aktuálnost dat
- Integrita a důvěryhodnost

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

2. Proč jsme do toho šli?

GDPR = sebevražedná mise; proč jdeme do toho dobrovolně?

1. IT centrum velké univerzity – mnoho inf-systémů
   - …dopadne to na nás tak-jako-tak
2. Když nebudeme aktivní, vymyslí to někdo jiný
   - …a nám se patrně to cizí řešení nebude líbit
3. Bezbřehá problematika
   - …někdo to musí koordinovat
   - …a DPO zatím nemáme

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

2.1 GDPR: Co v tom děláme?

- ÚVT MU – Divize kyberbezpečnosti a správy dat
- Koordinace na univerzitě
- Pilotní projekt FR CESNET
- Centralizovaný rozvojový projekt MŠMT 2018

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

2.1 GDPR: Co v tom děláme?

- ÚVT MU – Divize kyberbezpečnosti a správy dat
- **Koordinace na univerzitě**
  - Rozdělení zodpovědností:
    - Právní oblast
    - Technická oblast
    - Personální zajištění
- Pilotní projekt FR CESNET
- Centralizovaný rozvojový projekt MŠMT 2018

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

2.1 GDPR: Co v tom děláme?

- ÚVT MU – Divize kyberbezpečnosti a správy dat
- Koordinace na univerzitě
- **Pilotní projekt FR CESNET**
  - Od 2017/04, 5 partnerů
  1. Právní analýza dopadů GDPR na IT na VŠ
  2. Metodika DPIA – a její pilotní aplikace
  3. Informovanost (série seminářů spolu s CESNETem)
  4. Získání znalostí a zkušeností pro rozsáhlejší projekt
- Centralizovaný rozvojový projekt MŠMT 2018

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

2.1 GDPR: Co v tom děláme?

- ÚVT MU – Divize kyberbezpečnosti a správy dat
- Koordinace na univerzitě
- Pilotní projekt FR CESNET
- **Centralizovaný rozvojový projekt MŠMT 2018**
  - Všech 26 veřejných VŠ v ČR (projekt podán 31.10., MU koordinátor)
    1. Zajistit k 25.5.2018 soulad s GDPR v klíčových oblastech
    2. Ošetřit všechny zásadní systémy za zpracování OÚ
    3. Nasadit první verzi Komplexního řešení ochrany OÚ
    4. Základy pro dlouhodobou spolupráci VVŠ
  - Pracovní skupiny: Právo, Implementace, Inf-systémy, Výzkumná data

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. Personální zajištění
3. Metodiky
4. Registr činností zpracování OÚ
5. Posouzení dopadů
6. Realizace opatření
7. Dokumentace
8. Veřejná informace
9. Vzdělávání, školení

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

3. Komplexní systém ochrany OÚ na VŠ

1. **Interní legislativa**
   - Směrnice a pokyny upravující základní principy zpracování OU na dané VŠ (zodpovědnosti, povinnosti, postupy)
2. Personální zajištění
3. Metodiky
4. Registr činností zpracování OÚ
5. Posouzení dopadů
6. Realizace opatření
7. Dokumentace
8. Veřejná informace
9. Vzdělávání, školení

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. **Personální zajištění**
   - Zajištění potřebných personálních kapacit: pověřenec pro ochranu OÚ (DPO), právní podpora, metodik, …
3. Metodiky
4. Registr činností zpracování OÚ
5. Posouzení dopadů
6. Realizace opatření
7. Dokumentace
8. Veřejná informace
9. Vzdělávání, školení

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. Personální zajištění
3. **Metodiky**
   - Postupy a doporučení pro zodpovědné osoby, zaměstnance, uživatele v různých oblastech (weby, e-komunikace, ukládání dat, reakce na incidenty, …)
4. Registr činností zpracování OÚ
5. Posouzení dopadů
6. Realizace opatření
7. Dokumentace
8. Veřejná informace
9. Vzdělávání, školení

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. Personální zajištění
3. Metodiky
4. **Registr činností zpracování OÚ**
   - Přehled a základní dokumentace o všech činnostech zpracování OU v organizaci (povinnost dle GDPR)
5. Posouzení dopadů
6. Realizace opatření
7. Dokumentace
8. Veřejná informace
9. Vzdělávání, školení

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. Personální zajištění
3. Metodiky
4. Registr činností zpracování OÚ
5. **Posouzení dopadů**
   - Vyhodnocení rizik u jednotlivých zpracování OÚ v organizaci a návrh opatření k jejich eliminaci/snížení (DPIA)
6. Realizace opatření
7. Dokumentace
8. Veřejná informace
9. Vzdělávání, školení

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. Personální zajištění
3. Metodiky
4. Registr činností zpracování OÚ
5. Posouzení dopadů
6. **Realizace opatření**
   - Technická opatření (úpravy systémů) a organizační opatření pro jednotlivá zpracování OÚ (zabezpečení, vypořádání práv SÚ)
7. Dokumentace
8. Veřejná informace
9. Vzdělávání, školení

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. Personální zajištění
3. Metodiky
4. Registr činností zpracování OÚ
5. Posouzení dopadů
6. Realizace opatření
7. **Dokumentace**
   - Dokumentace všeho k prokázání, že organizace se tím zabývala a jak (záznamy z posouzení, smlouvy, souhlasy, závazky mlčenlivosti, proškolení)
8. Veřejná informace
9. Vzdělávání, školení

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. Personální zajištění
3. Metodiky
4. Registr činností zpracování OÚ
5. Posouzení dopadů
6. Realizace opatření
7. Dokumentace
8. **Veřejná informace**
   - Naplnění požadavku „transparentnosti“ – webová prezentace se zásadami ochrany OÚ v organizaci, kategoriemi zpracování OÚ, poučení pro SÚ, …
9. Vzdělávání, školení

3. Komplexní systém ochrany OÚ na VŠ

1. Interní legislativa
2. Personální zajištění
3. Metodiky
4. Registr činností zpracování OÚ
5. Posouzení dopadů
6. Realizace opatření
7. Dokumentace
8. Veřejná informace
9. **Vzdělávání, školení**
   - Vzdělávací a informační materiály plus systém proškolování pro všechny kategorie pracovníků (vedoucí pracovníky; tvůrce, správce a uživatele lsů, zaměstnance, …)

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

4. GDPR = analýza rizik. Ale kterých a jak?

- **GDPR**
  - Rizika pro práva a svobody SÚ
  - Vysoká rizika → opatření ke snížení/eliminace rizik → zbytková rizika →
- **Organizace**
  - Rizika ztráty prestiže a důvěryhodnosti
  - Rizika finanční
- **Otevřená společnost**
  - Rizika ztráty (přístupu/existence) doposud dostupných dat
  - Přehnaný alibismus, uzavírání, panika

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

4.1 Panika – příklady z praxe

- Fotografie/videa ze života organizace
- Docházková kniha
- Seznamy účastníků
- Rozvrhy na učebnách
- Jmenovky u kanceláří

- …a už to jede!

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

5. Fotografie v organizaci – jak na to?

Různé přístupy (mezi „mlýnskými kameny“)

- **Alibi nade vše**
  - Preventivně si vše sami zakážeme, přestaneme fotit, staré fotky zlikvidujeme…
- **Detailní metodika**
  - Přesně upravíme a podchytíme všechny možnosti – riziko vlastní pasti
- **Kašleme na to**
  - Nějak bylo, nějak bude. Předtím jsme to také neřešili, takže co…
- **Zdravý rozum**
  - Hledáme schůdnou variantu, jak to lze dělat bez velkých komplikací
  - Nesnažit se řešit naprosto vše (rámcové doporučení, vědomé šedé zóny)
  - Zpravodajská licence dle OZ (bez souhlasu), portrétní fotografie (souhlas)
    + zdravý rozum jako dosud: děti (pozor!), publikace, dehonestující záběry, …

https://www.smartinsights.com/marketplace-analysis/digital-marketing-laws/marketing-implications-of-the-eu-general-data-protection-regulation-gdpr/

ÚSTAV VÝPOČETNÍ TECHNIKY
Masarykova univerzita

DISKUSE

Kontakt:
Miroslav Bartošek
bartosek@ics.muni.cz