

Ochrana osobních údajů ve stínu AI

Ondřej Lešetický

POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ
JIHOČESKÉ CENTRUM KYBERNETICKÉ BEZPEČNOSTI, S.R.O.



Pověřenec pro ochranu osobních údajů | DPO



Monitorování souladu zpracování osobních údajů s GDPR.

Koordinace činností interní ochrany dat.

Školení pracovníků ve standardech/směrnicích pro zpracování dat organizace.

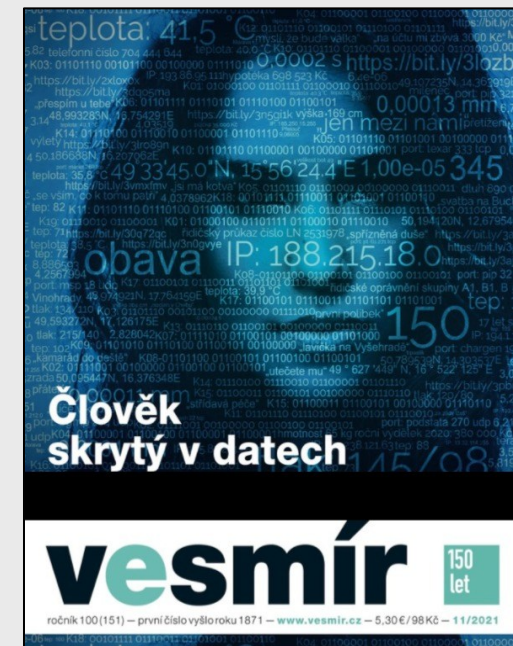
Provádění interních auditů organizace ve smyslu dodržování GDPR.

Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu.

Implementace GDPR (ve zdravotnictví)



- Souběh listinné a digitální podoby agend
- Heterogenní ICT prostředí!
- Zpracování výhradně dle čl. 6., odst. 1, písm. c), b), f)
- Zvláštní kategorie osobních údajů
 - zdravotní stav, genetické, biometrické
- Relevantní sektorová legislativa?



Trendy ve zdravotnictví



- Pokročilý medicínský software
- „Smart“ roboti
- 3D tisk
- Proliferace AIS napříč obory
 - *Relevantní legislativa v sektoru není jenom AI Act, ale také:*
 - MDR, IVDR, MDCG, EHDS, ...

Umělá inteligence se prosazuje i v českém zdravotnictví

7 minut čtení | 28. 3. 2024 | ač | Vyšlo v titulu [Medical Tribune](#)



Rizika aplikace AIS a jejich mitigace



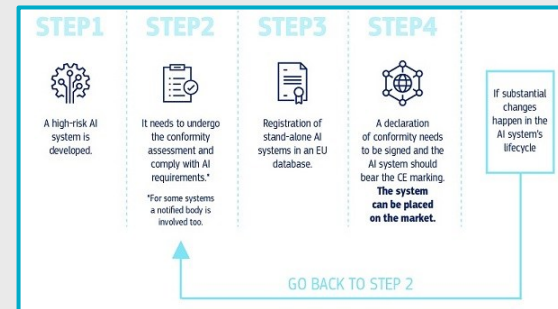
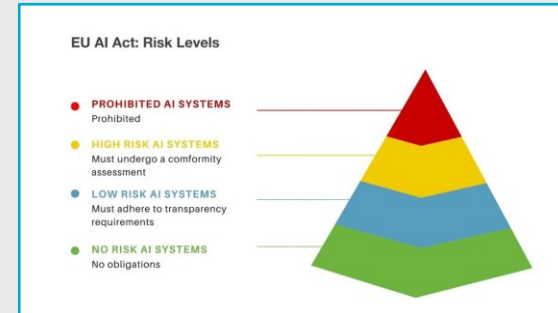
1. Rizika spojená s kvalitou dat
2. Rizika chybné diagnostiky a rozhodování
3. Kybernetická a bezpečnostní rizika
4. Etická a právní rizika
5. ..
6. Rizika AIS ve zdravotnictví z pohledu ochrany osobních údajů (GDPR)



Rizika aplikace AIS a jejich mitigace



1. AI/data governance, reprezentativní datasety
2. Princip *human-in-the-loop*
3. Testování a certifikace AIS
4. Šifrování dat, silná autentizace, bezpečnostní audity
5. Soulad s legislativou 😊
6. Systematické vzdělávání personálu
7. SLA, BCMS, *fall-back* scénáře



Rizika aplikace AIS a jejich mitigace



1. Důsledné vymezení účelu a právního základu pro zpracování
2. Klasifikace AIS, posouzení vlivu na ochranu osobních údajů (DPIA)
3. Principy *privacy by design/by default*
4. Testování zpětné korelace (re-identifikace)
5. Důsledná anonymizace, pseudonymizace
6. Transparentnost (aktualizace informací o zpracování)
7. Procesy uplatnění práv subjektu údajů (přístup-opravu-výmaz)
8. Human-in-the-loop
9. Šifrování, řízení přístupů, logování operací a pravidelné bezpečnostní audit.

AI ve zdravotnictví



Pacient
Anonymní Pacient, ostatní
ID: 129164

Studie
Číslo žádanky: PNF
Datum vyšetření: 15. 3. 2024 - 9:11:01
Datum zprávy: 15. 3. 2024
Popis studie: RTG - Plicie
Jazyk textu: Czech
Typ pozorovatele: Přístroj
Výrobce přístroje: CAREBOT
Název přístroje: Carebot AI CXR
Modelové číslo přístroje: 2.2.19
Ejštění: NÁLEZ

(Upozornění: Následující textový výstup je automaticky generován na základě výsledku analýzy snímku umělou inteligencí. Definitivní hodnocení snímku a lékařská zpráva musí být korelována s klinickými obrazy a zůstává odpovědností lékaře.)

Plicie: Na snímku jsou známký přítomnosti fluidothoraku. Jsou přítomny známký konsolidace plicního parenchymu. Bez známký atelektázy. Bez detekovaných ložiskových změn v rozsahu plicí. Plicní křídla jsou rozvinutá.
Srdce: Srdceň stín je hraniční šířky.
Ostatní: Bez známký podkožního emfyzému v zobrazeném rozsahu.

Rizikové skóre:
Zvětšení srdečního stínu (CMO): Zvýšené riziko
Fluidothorax (EFF): Vysoké riziko
Konsolidace plicního parenchymu (COM): Vysoké riziko
Atelektáza (ATE): Nízké riziko
Léza plicního parenchymu (LES): Nízké riziko
Pneumothorax (PMO): Nízké riziko
Podkožní emfyzém (SCE): Nízké riziko

Study Instance UID 1.2.826.0.1.3680043.8.1053.6.1539743610085.263.639896745

Carebot AI CXR je systém pro podporu rozhodování (zařazení „prediction, software that is intended to provide information for decision-making for diagnostic or therapeutic purposes“) na bázi počítačové podporované detekce. Software Carebot AI CXR je certifikován v souladu s požadavky Nařízení Evropského parlamentu a Rady (EU) 2017/745 (MDR) oznámeným subjektem NB 1023 (Institut pro testování a certifikaci, s. r. o.). Software Carebot AI CXR může obsluhovat pouze zaškolení personál s požadovanou způsobilostí. Vyhodnocování snímků lze provádět pouze na certifikovaných radiologických monitorech a v souladu s doporučením výrobce. Před užitím je nutné seznámit se s návodem k použití. V případě obdržení nesprávného výsledku prosím kontaktujte report@carebot.com pro předání zpětné vazby.

Čtěte návod k použití na odkaze
[redacted]

Carebot s.r.o.
Kozdrojovice 246
664 34 Kozdrojovice

Závěry



- Ochrana osobních údajů představuje jeden z klíčových aspektů při zavádění AIS ve zdravotnictví. Dodržování principů GDPR, spolu s implementací technických a organizačních opatření, je nezbytné pro zajištění důvěry pacientů i právní *compliance* zdravotnických institucí.
- AI a GDPR v roce 2026: HR, EHDS a nový Digital Omnibus.





Děkuji za pozornost