DECT

MUNI LAW

Národní centrum kompetence pro kyberbezpečnost

e4j

GDPR, AI A KYBERNETICKÁ OBRANA

VÁCLAV STUPKA

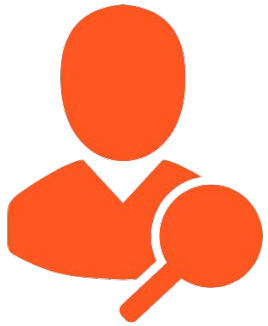
OCHRANA OSOBNÍCH ÚDAJŮ

PRÁVNÍ ÚPRAVA

- Nařízení EU č. 2016/679, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
- První návrh – leden 2012
- Těžká lobby - 4 roky ladění, 3000 změnových návrhů
- Účinnost – 25. května 2018

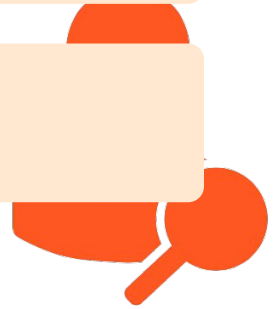
NAŘÍZENÍ

- Vlastní čtení nenahradíš: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=consil:ST_5419_2016_INIT
- 200 stran (ale polovina je předmluva)



HLAVNÍ PRINCIPY

- Velmi podobná podstata právní úpravy jako dříve
- Co není dovoleno, to je zakázáno (vyjmenované důvody pro zpracování)
- Obecné kategorie pro posuzování compliance
- Dokumentace, dokumentace, dokumentace

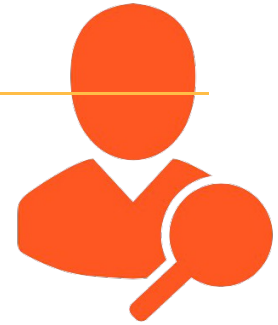


POJMY

Osobní údaje	Subjekt údajů	Zpracování
Správce	Zpracovatel	Účel a prostředky zpracování

DŮVODY ZPRACOVÁNÍ

- Souhlas subjektu údajů
- Smluvní závazek
- Právní povinnost
- Ochrana životně důležitých zájmů subjektu nebo FO
- Veřejný zájem/výkon veřejné moci
- Oprávněný zájem správce/třetí osoby



#1 - NAŘÍZENÍ, NIKOLIV SMĚRNICE!

- Přímo účinná norma
- Není třeba implementace (ale)
- Nahrazuje národní právní úpravu

#2 – VZTAHUJE SE NA HODNĚ KATEGORIÍ DAT

- Směřuje k ochraně osobních údajů
- Co online identifikační prvky (IP adresy, UDID)?
- Pseudonymizace k čemu ?

OSOBNÍ ÚDAJE

- *“veškeré informace o (přímo či nepřímo) identifikované nebo identifikovatelné fyzické osobě”*
  - identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby

PSEUDONYMNÍ ÚDAJE

- Nejsou přímo spojena se subjektem (ale mohou být)

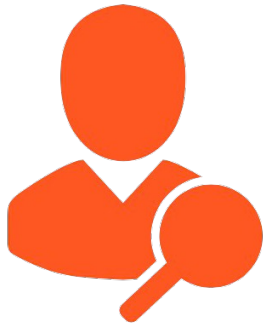
- Volnější pravidla:
  - Oznamování
  - Profiling
  - Přístup subjektu údajů

#3 – JE EXTRATERITORIÁLNÍ

- Dříve se úprava vztahovala jen na subjekty v rámci EU/EHS.

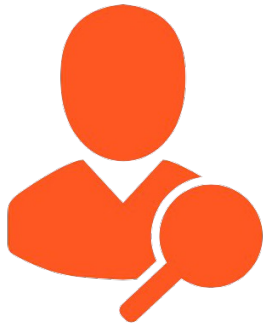
- Nyní pravidla platí když:
  - Sídlo v EU
  - Nabízení služeb EU rezidentům
  - Monitorování chování EU rezidentů

- Vztahuje se tedy I na subjekty mimo EU!



ZÁSTUPCE V EU

- Správci a zpracovatelé neusazení v EU
  - Jmenují zástupce v jednom z členských států
  - Zmocněn k zastupování
  - Správce/zpracovatel stále odpovědný



#4 - VZTAHUJE SE NA ZPRACOVATELE

- Dříve žádné povinnosti zpracovatele (např. poskytovatelé služeb)

- GDPR = jasná odpovědnost a povinnosti zpracovatele
- Závazná ustanovení smluv
- Správce musí hodnotit kvalitu zpracovatele

- Výrazný dopad na cloudové služby?

POVINNOSTI ZPRACOVATELE

uchovávání informací

jaká data,
jaké zpracování,
kde data jsou,
technická zabezpečení,

ohlášení porušení zabezpečení

USTANOVENÍ SMLUV

- Zpracování jen na pokyn správce,
- dostatečné zabezpečení,
- bezpečnost subdodavatelů,
- mlčenlivost,
- nápomoc správci při výkonu práva subjektu,
- vymazání a vrácení dat
- postupy prokazování compliance

#5 – VĚTŠÍ DŮRAZ NA ODPOVĚDNOST

- “Vhodné” nástroje k prokázání compliance
- Mohou zahrnovat:
  - Zaznamenávání detailů o zpracování
  - Zavedení bezpečnostních opatření
  - Studie dopadu (DPIA)
  - Osvědčení, Kodexy chování
  - Privacy-by-design, Privacy-by-default
  - Pověřenec pro ochranu OÚ
- Není třeba se registrovat

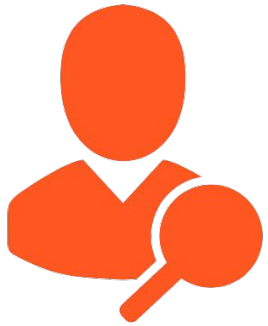
DETAILY O ZPRACOVÁNÍ

- Označení správce
- Účely zpracování
- Kategorie subjektů a údajů, příjemců
- Lhůty pro výmaz
- Dokumentace bezpečnostních opatření

BEZPEČNOSTNÍ OPATŘENÍ

- *“S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob”*

- Demonstrativní výčet nástrojů:
  - Pseudonymizace, šifrování
  - CIA triáda systémů
  - Zálohování
  - Revize ochrany



DPIA

- Nutné:
  - automatizované rozhodování s významným dopadem,
  - rozsáhlé zpracování zvláštních kategorií OÚ
  - rozsáhlé monitorování veřejných prostor
- Jinak doporučeno v případě reálného rizika
- Obsah:
  - Popis účelů a mechanismů zpracování
  - Nezbytnost a přiměřenost operací
  - Posouzení rizik
  - Plánovaná opatření

KODEXY CHOVÁNÍ, PODNIKOVÁ PRAVIDLA

Kodexy:

Sdružení a zástupci kategorií správců

Zpřesňuje postupy při zajištění compliance

Schvaluje dozorový úřad

Plnění monitorují akreditované subjekty

Osvědčení:

Prokazuje compliance správce

Vydává akreditovaný subjekt

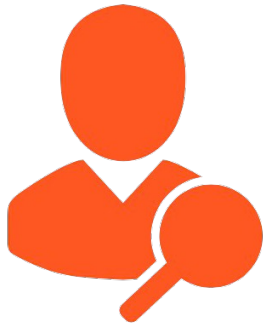
ZÁMĚRNÁ A STANDARDNÍ OCHRANA OSOBNÍCH ÚDAJŮ

- Dle stavu techniky
- Technická a organizační opatření
- Cíl:
  - Minimum zásahu
  - Minimum zpracovávání
  - Minimum údajů

#6 – POSÍLENÍ PRÁV SUBJEKTU ÚDAJŮ

- Existující práva: přístup, oprava, smazání a blokování

- Posílení:
  - Jednoznačný souhlas
  - Posílení práv na přístup a námitku
  - Přímo zahrnuje právo na zapomění
  - Přenositelnost údajů
  - Ochrana proti profilování



SOUHLAS

- Prokazuje správce
- Samostatný a srozumitelný
- Snadné odvolání
- Zvláštní pravidla pro subjekty mladší 16 (13) let

PŘÍSTUP

- Informace o zpracování
  - Účely zpracování
  - Kategorie údajů
  - Příjemci
  - Doba uchování
  - Existence práva na výmaz, omezení, námitku či stížnost
  - Informace o zdroji
  - Profilování/automatizované rozhodování

PRÁVO NA OPRAVU, VÝMAZ

- Výmaz:
  - Zánik účelu
  - Odvolání souhlasu
  - Námitka
  - Protiprávní zpracování
  - Právní povinnost

PŘENOSITELNOST ÚDAJŮ

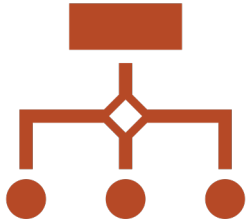
- Podmínky: souhlas/smlouva, automatizované zpracování
- Právo získat a předat údaje jinému správci
- Strukturovaný a strojově čitelný formát
- Přímé předání

PROFILOVÁNÍ/AUTOMATIZOVANÉ ROZHODOVÁNÍ

- *“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.”*

- Výjimky: nezbytnost k uzavření/plnění smlouvy, právem dovoleno, souhlas subjektu

#7 – OZNAMOVÁNÍ NARUŠENÍ BEZPEČNOSTI



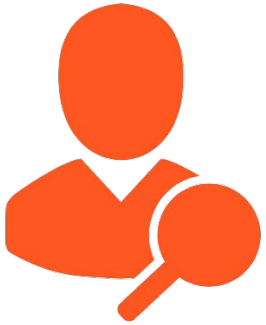
Oznamuje se:

Správci (jste-li zpracovatel)

Dozorovému úřadu

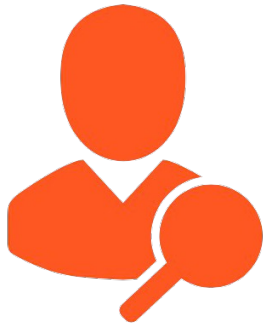
Subjektu (ne je-li dopad malý)

Obecně do 72 hodin



OZNAMOVÁNÍ

- Subjektu:
  - je-li vysoké riziko
  - Ne, zajistil-li správce nápravu, nebo není prakticky možné
- Úřadu:
  - Jakékoliv porušení
  - Hlásí se:
    - Povaha porušení zabezpečení,
    - kategorie a počet subjektů a údajů,
    - kontakt na pověřence,
    - důsledky,
    - přijatá opatření

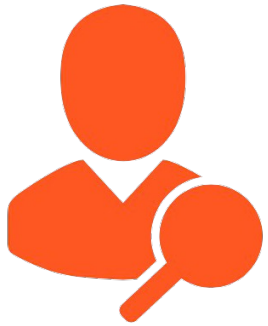


#8 – POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

- Současné právo nezná
- Nový požadavek na správce i zpracovatele

- Kdy?
  - Veřejnoprávní autorita nebo subjekt
  - “rozsáhlé” systematické monitorování osob
  - “rozsáhlé” zpracování citlivých dat

- Může jít o zaměstnance nebo outourcovanou službu



POSTAVENÍ POVĚŘENCE

- Jmenován správcem/zpracovatelem
- Zapojen do všech aktivit s vlivem na osobní údaje
- Nezávislý, chráněn, povinnost mlčenlivosti
- Úkoly:
  - Poskytování rad a návodů
  - Monitoring compliance
  - Spolupráce s úřadem

#9 – PROBLEMATICKÉ PŘEDÁVÁNÍ DAT

- V současnosti je velmi omezeno předávání do třetích zemí

- Koncept odpovídající ochrany
- Koncept vhodných záruk
- Povolení

#10 - POKUTY

- Až € 20 M, až 4% celosvětového obratu
- Audity dozorových úřadů
- Nové správní nástroje (stížnost, žaloba)
- One stop shop

UMĚLÁ INTELIGENCE

CÍLE AKTU O AI

BEZPEČNOST A OCHRANA PRÁV

PODPORA INOVACÍ

ZAJIŠTĚNÍ PRÁVNÍ JISTOTY

ZÁKLADNÍ CHARAKTER

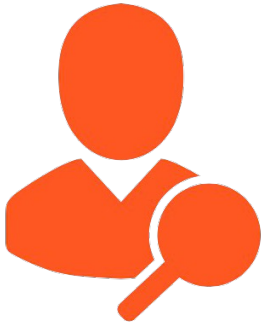
- Snaha o technologickou neutralitu a regulatorní flexibilitu
- Specifická legislativa s vědomím celkového regulatorního kontextu
- Očekávaná návazná sektorově specifická regulace a standardy
- Postaveno na analýze rizik a compliance

ZÁKLADNÍ DEFINICE A ROZSAH

- AI: velmi široká definice zahrnující všechny možné techniky AI – nejedná se jen o ChatGPT nebo velké jazykové modely
- Rozsah aplikace:
- **Geograficky**: všichni poskytovatelé a uživatelé AI v i mimo EU, využívá-li se příslušné AI v EU
- **Sektorově**: různé aplikace AI v širokém spektru sektorů se zaměřením na kritické – doprava, finanční sektor
- **Technologicky**: jakékoliv existující i budoucí systémy spadající pod definici

ZÁKLAD V ANALÝZE RIZIK

- Analýza rizik předchází implementaci požadavků
- Hodnotí se úroveň rizika pro bezpečnost a základní práva
- Cílem je dosažení proporcionality restriktivních pravidel
- Posuzované faktory analýzy rizik:
- Způsob a rozsah využití AI
- Sektor, ve kterém je AI využívána
- Potenciální dopad na práva a svobody jednotlivců



ÚROVNĚ RIZIKA

- Nepřijatelné riziko: Využití AI pro manipulaci lidského chování za účelem potlačení svobodné vůle, social scoring
- Vysoké riziko: Využití AI v kritické infrastrukture, vzdělávání, zaměstnávání, základních veřejných a soukromých službách
- S požadavkem na transparenci: AI systémy interagující s lidmi (např. chatboty)
- Minimální riziko: ostatní

ZAKÁZANÉ PRAKTIKY

Manipulace a zneužití AI: manipulace za účelem potlačení svobodné vůle, zneužití zranitelností skupin osob (věk, postižení, sociální postavení apod.)

Sociální scoring: využití k vyhodnocování důvěryhodnosti a kvality osob na základě profilování a predikce osobních charakteristik směřující k omezení práv

Vzdálená biometrická identifikace v reálném čase: masové sledování pro vymáhání práv na základě biometrie je zakázané, není-li za účelem vyhledání poškozených, předcházení bezprostředním hrozbám, lokalizace a identifikace pachatelů

Ochrana základních práv: Techniky využití AI pro omezení lidských práv a svobod (soukromí, nediskriminace, osobní údaje apod.)

VYSOKÉ RIZIKO

- **Kritická infrastruktura**: správa kritických infrastruktur
- **Vzdělávání**: hodnocení studentů s vlivem na jejich příležitosti
- **Zaměstnávání**: hodnocení uchazečů o práci a zaměstnanců
- **Základní služby**: rozhodování o přístupu k základním službám
- **Trestní řízení**: prediktivní a monitorovací systémy zasahující do lidských práv
- **Migrace, azylová řízení**: zpracování podkladů pro rozhodování orgánů
- **Justice**: automatizace v justici a rozhodovací praxi, systémy zasahující do demokratického procesu
- **Bezpečnostní komponenty produktů**: např. zdravotnická zařízení, hračky

POŽADAVKY

Vysoké riziko

- **Komplexní posouzení rizik** již před nasazením
- **Data management**: dokumentace kvality dat využitých k učení, testování a validaci systémů
- **Dokumentace:** vedení dokumentace o vývoji, provozu a nasazení AI, dokumentace funkcionalit a účelů, za účelem ověření shody s požadavky aktu
- **Transparence a informační povinnosti**: Informační povinnosti vůči uživatelům ohledně schopností a omezení technologie a očekávané spolehlivosti výsledků
- **Lidský dohled**: u systémů dohlížejících na lidskou aktivitu musí být možnost revize rozhodnutí člověkem, zvlášť v kritických situacích, za účelem snížení rizik
- **Robustnost a bezpečnost**: musí být dokumentována opatření k zajištění robustnosti a bezpečnosti systémů AI
- **Posouzení shody**: před nasazením systému musí být zpracováno posouzení shody s požadavky – v některých případech při využití testování a hodnocení třetími osobami
- **Registrace**: systémy s vysokým rizikem budou evidovány v databázi EU

POSTUP APLIKACE

Vysoké riziko

Identifikace úrovně rizika → Design a vývoj v souladu s požadavky, dokumentace → Procedura posouzení shody → Označení CE → Umístění na trh EU

OMEZENÉ RIZIKO

Specifické závazky k transparenci

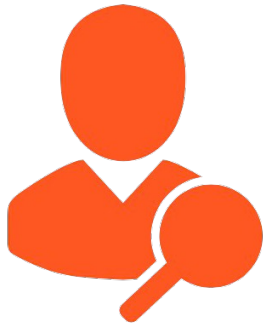
- **Chatboty**: AI systémy poskytující informace nebo služby osobám
- **Obsah generovaný AI**: systémy vytvářející či manipulující obsah (obrázky, videa, text apod.)
- **Personalizační algoritmy**: algoritmy personalizující obsah sociálních sítí a služeb podle uživatelského chování

- Výzvou bude nastavení hranic mezi omezeným rizikem a vyššími stupni rizika.

POŽADAVKY

Specifické závazky k transparenci

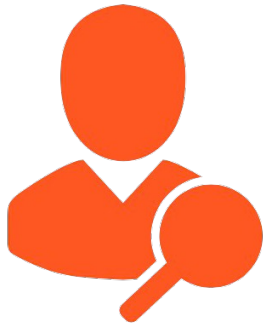
- **Transparentnost**: uživatelé musí být informováni o tom, že interagují s AI a o tom jaké funkce vykonává
- **Informace o obsahu generovaném AI**: obsah generovaný AI musí být označen a uživatel informován o povaze vytvořeného obsahu a jeho limitech
- **Labeling deepfaků**



NÍZKÉ RIZIKO

Minimální/nulové riziko

- Zahrnuje všechny ostatní kategorie využití AI, které nespadají do vyšších úrovní.
- Neuplatňují se žádné závazné požadavky
- Budou vytvářena nezávazná pravidla, která mohou dobrovolně uplatňovat provozovatelé low-risk systémů.



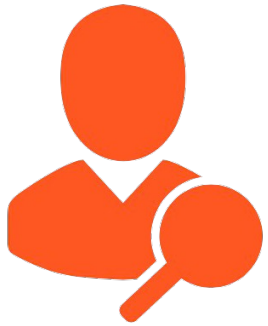
REGULATORNÍ PÍSKOVIŠTĚ

- AI act počítá s tím, že by na úrovni členských států mohly vznikat tzv. Sandboxy:
- Možnost simulace využití AI v různých aplikacích
- Dohled autority, možnosti konzultací
- Využití sítě EDIH
- Sektorově specifické sandboxy mohou vznikat i v high-risk oblastech

KYBERNETICKÁ OBRANA

POJEM KYBERNETICKÉ OBRANY

- Využití bezpečnostních nástrojů k předcházení, zastavení nebo odvrácení kybernetického útoku ohrožujícího zajišťování obrany státu
- Různá chápání:
  - NATO,
  - USA,
  - Rusko,
  - EU…



KYBERNETICKÁ OBRANA V ČR

- Gesce: VZ – Národní centrum kybernetických operací (NCKO)
- Spolupráce – AČR, zpravodajské služby (BIS, ÚZSI)
- Utajené postupy – budování kapacit
- Kromě toho ochrana vlastních infrastruktur – MO/AČR

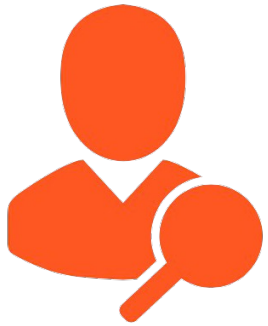
KYBERNETICKÁ OBRANA - ZOVZ

- Pravomoci VZ
  - Detekce
  - Vyhodnocování
  - Opatření k odvracení

- Spolupráce s různými relevantními subjekty:
  - Při provádění činností a opatření
  - Při detekci s podnikateli podle ZoEK (na základě dohody, povinně v případě rizika prodlení)

Informační povinnost, inspektor

Náhrada škody a nemajetkové újmy



DETEKCE

- Možnost instalace vlastních zařízení pro detekci v komunikačních sítích (není-li možné uzavřít dohodu, nebo tato není efektivní)
- Zaznamenávaná metadata:
  - popisující **informace a souvislosti nezbytné pro přenos dat, jejich strukturu a čas o zachyceném provozu v telekomunikacích**, a to pouze **v rozsahu souvisejícím s detekovaným kybernetickým útokem nebo hrozbou** na základě stanovených ukazatelů; **součástí není obsah přenášených dat**
  - Provozu detekčního nástroje a o manipulaci s ním
- Negativní vymezení: odposlech, aktivní zásah
- Nutnost zachování CIA triády telekomunikací
- Nesmí být zasahováno do činnosti subjektů podle ZoEK
- ISP povinnost vytvořit rozhranní pro připojení zařízení pro detekci
  - (na základě rozhodnutí MO, lhůty, náhrada nákladů)

OPATŘENÍ

- Na základě výsledku vyhodnocení detekovaných útoků nebo hrozeb
  - Předání informace relevantním státním orgánům, Národnímu CERTU, případně subjektu schopnému reakce na útok nebo hrozbu (nejsou-li naplněny podmínky aktivního zásahu)
  - Hrozí-li prodlení -> aktivní zásah
- Podmíny pro realizaci aktivního zásahu:
  - Existence ohrožení důležitých zájmů státu ve značném rozsahu
  - Útok nebo hrozba bezprostředně hrozí nebo trvá
  - Nelze odvrátit ve spolupráci s ozbrojenými silami a aktivní zásah je jediná možnost
  - Souhlas ministra obrany

INFORMAČNÍ POVINNOSTI

- Předávání informací o aktivním zásahu
  - O zahájení: vládu, NÚKIB a zpravodajské služby
  - O provedení: ministr obrany -> vláda, náčelník GŠ, ředitel NÚKIB, ostatní zpravodajské služby, v nezbytném rozsahu Národní CERT
- Obecně informace a součinnost pro NÚKIB a Policii ČR v rozsahu jejich působnosti
- Předání dat a realizace aktivních zásahů se eviduje
- Zpráva o činnosti – vláda a prezident (ročně)
- Zpráva o plění úkolů – ministr obrany (pololetně)

INSPEKTOR PRO KYBERNETICKOU OBRANU

- Jmenuje vláda na 5 let, voják VZ podřízen ministrovi obrany
- VZ – poskytuje informace, přístup, materialní a personální vybavení
- Vypracovává zprávu o nedostatcích a návrhy na zlepšení ministrovi obrany
- Povinnosti:
  - Prověřuje správnost postupů VZ
  - Ověřuje účinnost bezpečnostních opatření, navrhuje jejich aktualizaci
  - Poskytuje poradenství v oblasti ochrany dat a informací
  - Spolupracuje v oblasti bezpečnosti s povinnými osobami
  - Obrací se na něj ISP při obavě o bezpečnost (podnět) – řešení podateli a PS

DÍKY ZA POZORNOST

STUPKA@NC3.CZ