DECT

MUNI LAW

Národní centrum kompetence pro kyberbezpečnost

e4j

OCHRANA OSOBNÍCH ÚDAJŮ

VÁCLAV STUPKA

PROČ?

Data protection directive – 1995

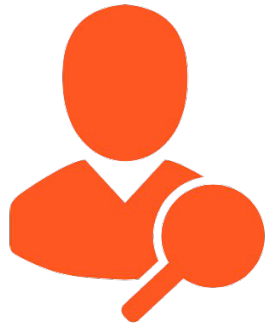
Nástup internetu, sociálních sítí, online služeb

Kompletní proměna technologického prostředí

Unifikace ochrany a nakládání s osobními údaji

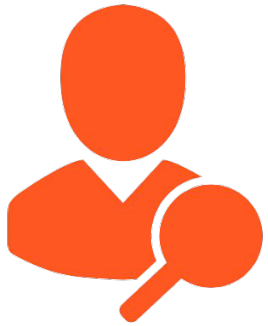
PRÁVNÍ ÚPRAVA

- 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



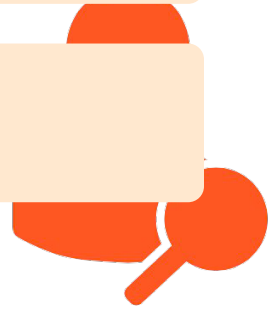
NAŘÍZENÍ

- 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

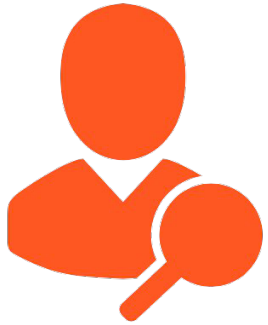
Osobní údaje	Subjekt údajů	Zpracování
Správce	Zpracovatel	Účel a prostředky zpracování

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

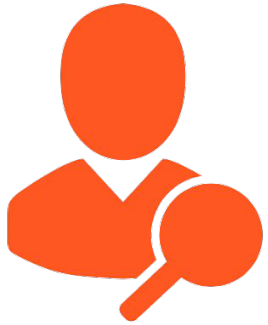
#1 - NAŘÍZENÍ, NIKOLIV SMĚRNICE!

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



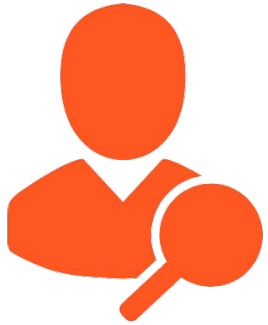
OMEZENÁ “IMPLEMENTACE”

- GDPR jako švýcarský sýr
- Cca 50 ustanovení umožňujících rozdílnou interpretaci členských států
- Je podstatné sledovat českou legislativu



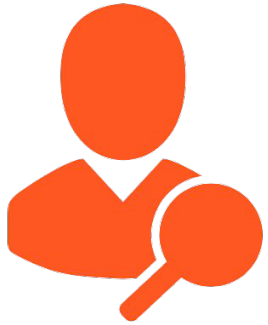
#2 – VZTAHUJE SE NA HODNĚ KATEGORIÍ DAT

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



OSOBNÍ ÚDAJE

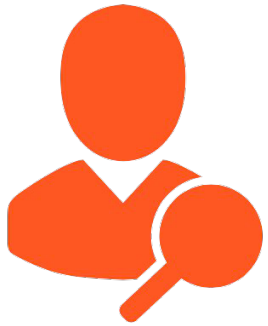
- *“veškeré informace o (přímo či nepřímo) identifikované nebo identifikovatelné fyzické osobě”*
  - identifikovatelnou fyzickou osobou je fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor 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

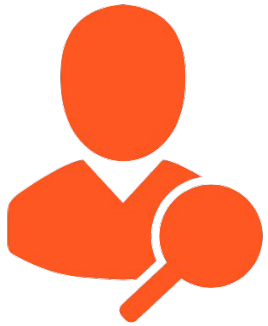


#3 – JE EXTRATERITORIÁLNÍ

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

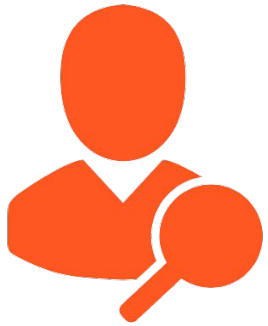
- Nyní pravidla platí když:
  - Sídlo v EU
  - Nabízení služeb EU rezidentům
  - Monitorování chování EU rezidentů

- 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

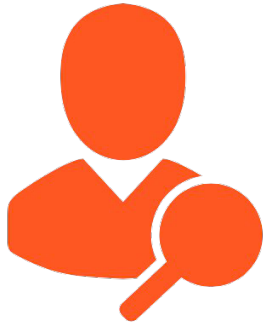


#4 - VZTAHUJE SE NA ZPRACOVATELE

- 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

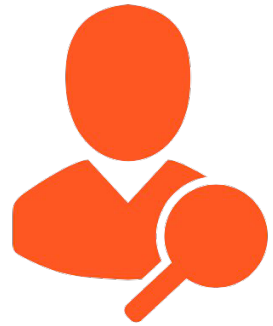
uchovávání informací

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

ohlášení porušení zabezpečení

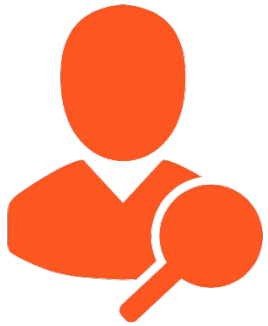
USTANOVENÍ SMLUV

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



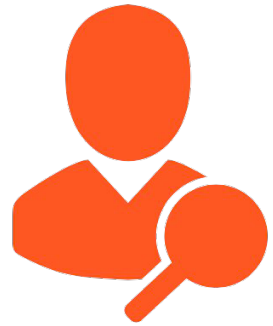
#5 – VĚTŠÍ DŮRAZ NA ODPOVĚDNOST

- “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

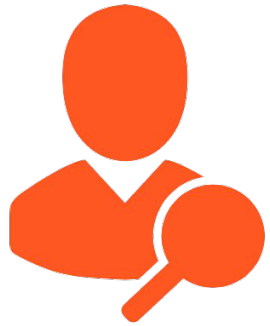
- Označení správce
- Účely zpracování
- Kategorie subjektů a údajů, příjemců
- Lhůty pro výmaz
- Dokumentace bezpečnostních opatření



BEZPEČNOSTNÍ OPATŘENÍ

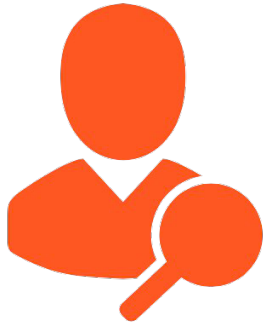
- *“S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob”*

- 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

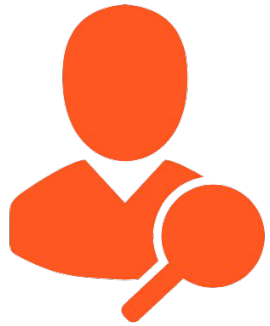
Osvědčení:

Prokazuje compliance správce

Vydává akreditovaný subjekt

ZÁMĚRNÁ A STANDARDNÍ OCHRANA OSOBNÍCH ÚDAJŮ

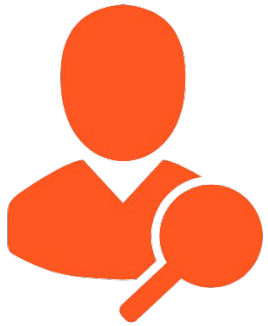
- Dle stavu techniky
- Technická a organizační opatření
- Cíl:
  - Minimum zásahu
  - Minimum zpracovávání
  - Minimum údajů



#6 – POSÍLENÍ PRÁV SUBJEKTU ÚDAJŮ

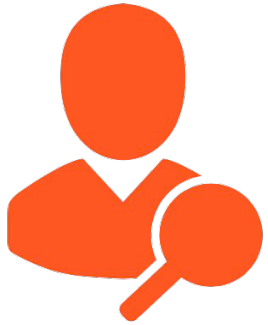
- Existující práva: přístup, oprava, smazání a blokování

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



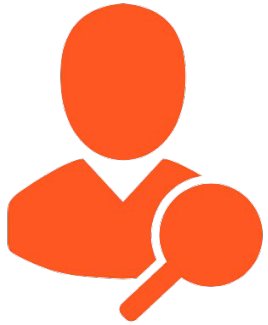
SOUHLAS

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



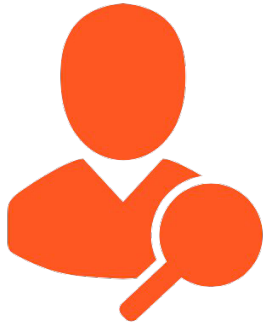
PŘÍSTUP

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



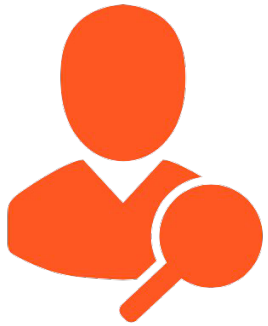
PRÁVO NA OPRAVU, VÝMAZ

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



PŘENOSITELNOST ÚDAJŮ

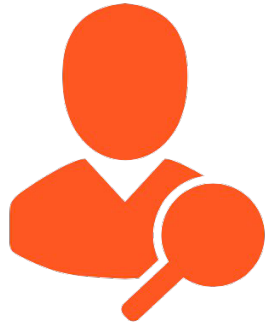
- Podmínky: souhlas/smlouva, automatizované zpracování
- Právo získat a předat údaje jinému správci
- Strukturovaný a strojově čitelný formát
- Přímé předání



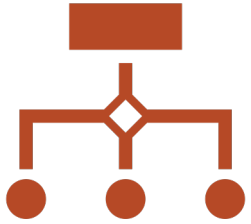
PROFILOVÁNÍ/AUTOMATIZOVANÉ ROZHODOVÁNÍ

- *“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



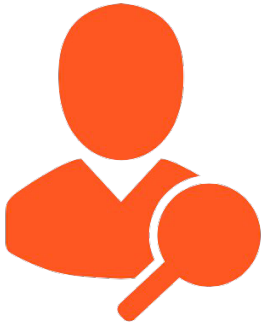
Oznamuje se:

Správci (jste-li zpracovatel)

Dozorovému úřadu

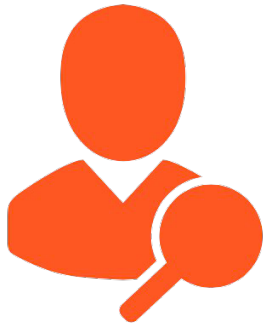
Subjektu (ne je-li dopad malý)

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

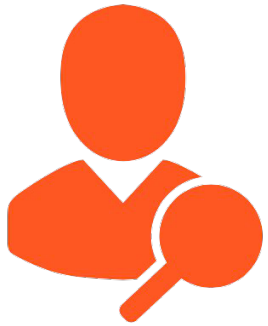


#8 – POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

- Současné právo nezná
- Nový požadavek na správce i zpracovatele

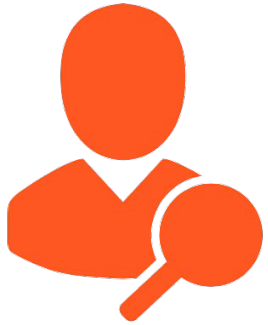
- Kdy?
  - Veřejnoprávní autorita nebo subjekt
  - “rozsáhlé” systematické monitorování osob
  - “rozsáhlé” zpracování citlivých dat

- Může jít o zaměstnance nebo outourcovanou službu



POSTAVENÍ POVĚŘENCE

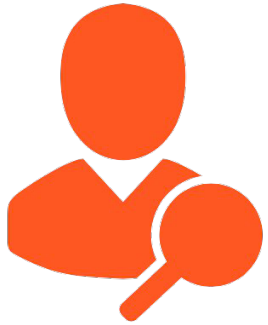
- Jmenován správcem/zpracovatelem
- Zapojen do všech aktivit s vlivem na osobní údaje
- Nezávislý, chráněn, povinnost mlčenlivosti
- Úkoly:
  - Poskytování rad a návodů
  - Monitoring compliance
  - Spolupráce s úřadem



#9 – PROBLEMATICKÉ PŘEDÁVÁNÍ DAT

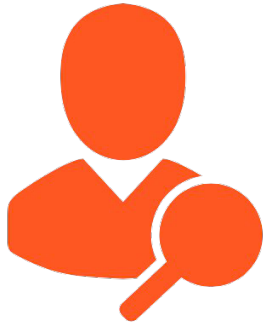
- V současnosti je velmi omezeno předávání do třetích zemí

- 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



DÍKY ZA POZORNOST

STUPKA@NC3.CZ