GDPR - půl roku poté
aneb dopady, změny, problémy při jeho aplikaci

FAKULTA INFORMATIKY

Katedra počítačových systémů a komunikací

RNDr. Karel Neuwirt

4. prosince 2018

Před 65 lety – 3. 9. 1953 vstoupila v účinnost

Úmluva na ochranu lidských práv a základních svobod (známá jako Evropská úmluva o lidských právech, ETS No. 5)

Convention 108 +

Convention for the protection of individuals with regard to the processing of personal data

www.coe.int/dataprotection

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Modernised Convention for the Protection of Individuals with Regard to the Processing of Personal Data (CETS No. 223)

Modernizovaná Úmluva 108 byla přijata Výborem ministrů Rady Evropy u příležitosti 128. zasedání, které se konalo v Elsinore (DK, 18 May 2018)
(ČR podepsala 10. 10. 2018)

Na základě „Úmluvy 108+", která má více než padesát smluvních stran, bude modernizovaná Úmluva nadále otevřena všem zemím světa jako jedinečný globální standard

Základní práva na soukromí a ochranu osobních údajů se stala důležitějšími pro ochranu lidské důstojnosti než kdykoli dříve

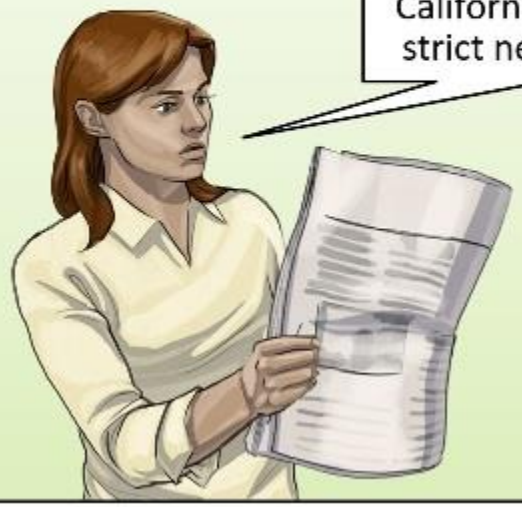
Umožňují jednotlivcům rozvíjet svou vlastní osobnost, vést samostatný život, inovovat a uplatňovat další práva a svobody

Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 **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) - též „GDPR“

Platnost: 25. 5. 2016 Účinnost: 25. 5. 2018

Úřední věstník Evropské unie L119, 4. května 2016

2018



2017

2016

2015, 2014, 2013 . . .

Written by Daniel J. Solove
Illustrated by Ryan Beckwith

'GDPR is one of the best things to happen for data security,' says CIO roundtable

A CIO roundtable states that the EU's General Data Protection Regulation has helped focus board minds on security

GDPR has a negative impact on venture investment and the advertising market in Europe

Computing's IT Leaders Summit, Oct., 2018

Významným pozitivním přínosem GDPR z pohledu byznysu a je tzv. „přístup na základě rizik“ (risk-based approach)

= zatímco stanovená pravidla jsou stejná pro všechny, jejich aplikace v praxi je rozmanitá a závisí na úrovni rizika, které dané zpracování vytváří vůči soukromí jedinců

GDPR - přístup založený na analýze rizik

povaha

účel

kontext

rozsah

Pravděpodobnost a míra rizika vyplývá z

povahy, **rozsahu**, **kontextu a účelu**

zpracování

klíčový faktor při posuzování souladu zpracování s Nařízením

Obecné nařízení o ochraně osobních údajů (**G**eneral **D**ata **P**rotection **R**egulation) platí pro všechny, kteří jakkoliv nakládají (zpracovávají) osobní informace o jednotlivcích v EU

Nařízení je platné od května 2016 a nabude účinnosti od 25. května 2018

Aplikovatelnost Nařízení nevyžaduje přijetí jakékoliv další legislativy členského státu

Pokud organizace neprokáže, že při nakládání s osobními údaji zajišťuje náležité úsilí pro docílení souladu s GDPR, pak se vystavuje riziku dozorové činnosti a odpovídajícím sankcím

Jelikož GDPR je zaměřeno na (osobní) „údaje“, vzniká mylný dojem, že celá problematika se týká především otázek informačních technologií (IT)

Avšak GDPR je změna celkové kultury zpracování údajů v organizaci (od získávání údajů, přes jejich používání, uchovávání či předávání dalším uživatelům)

Nařízení chrání základní práva a svobody fyzických osob, a zejména jejich právo na ochranu osobních údajů

Soudní dvůr EU

právo na ochranu osobních údajů není právem absolutním -

musí být posuzováno v souvislosti se svou funkcí ve společnosti a v souladu se zásadou proporcionality, musí být v rovnováze s dalšími základními právy

Nařízení respektuje všechna základní práva a dodržuje zásady uznávané Listinou základních práv Evropské unie, zejména právo na:

- respektování soukromého a rodinného života, obydlí a komunikace,
- ochranu osobních údajů,
- svobodu myšlení, svědomí a náboženského vyznání,
- svobodu projevu a informací,
- svobodu podnikání,
- účinný opravný prostředek a spravedlivý proces,
- kulturní, náboženskou a jazykovou rozmanitost

„Stručně řečeno, **zdravý rozum** není pramenem práva. Avšak výklad by se jím měl určitě řídit. Bylo by nanejvýš nešťastné, kdyby se ***ochrana*** osobních údajů měla přeměnit na ***obstrukci*** prostřednictvím osobních údajů.“

GENERÁLNÍ ADVOKÁT CJEU MICHAL BOBEK ve svém Stanovisku ve Věci C-13-16, předneseném dne 26. ledna 2017

Nebezpečí
při uplatňování zásad a pravidel GDPR v praxi

velmi široký výklad

aplikační absolutismus

Z toho, že navrhovaný prováděcí zákon ČR nebyl přijat k stejnému datu jako GDPR, jsou často vyvozovány nepodložené spekulace

ÚOOÚ proto připomíná, že **podstata** regulace ochrany osobních údajů je v **obecném nařízení**, neboť navrhovaný **zákon pouze upřesňuje** některé vybrané případy zpracování osobních údajů, které GDPR připouští

Členské státy mají možnost upřesnit uplatňování pravidel o ochraně údajů v konkrétních oblastech:

- veřejný sektor
- zaměstnanost a sociální zabezpečení
- preventivní a pracovní lékařství, veřejné zdraví
- účely archivace ve veřejném zájmu nebo pro vědecké, historické či statistické použití
- vnitrostátní identifikační číslo
- přístup veřejnosti k úředním dokumentům
- povinnost mlčenlivosti

V l á d n í n á v r h

ZÁKON

ze dne …… 2018

o zpracování osobních údajů

3. čtení v PS PČR přerušeno
pokračování navrženo na pořad 24. schůze (od 4. 12. 2018)

Subjekt údajů

Osobní údaj

Nové definice

osobní údaje - veškeré informace **o** identifikované nebo identifikovatelné fyzické osobě – „subjektu údajů“

(nyní: **o** *dříve:* týkající se, vztahující se; C108+ však používá „relating to“*)*

identifikovatelnou osobou je osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor - *např. jméno, identifikační číslo, lokalizační údaje, elektronický identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo sociální identity této fyzické osoby*

subjekt údajů - **identifikovaná fyzická osoba nebo FO, kterou lze přímo nebo nepřímo**, *samotnou či ve spojení s přiřazenými údaji*, **identifikovat nebo zjistit prostředky, o nichž lze rozumně (důvodně) předpokládat, že je správce … použije pro identifikaci dané osoby, zejména s odkazem na** *jedinečný identifikátor* **…..**

Při určování, zda je FO identifikovatelná nutno přihlížet ke všem prostředkům, o nichž lze rozumně předpokládat, že je správce nebo jiná osoba použijí pro přímou nebo nepřímou identifikaci FO
Rozumně předpokládat – vzít v úvahu objektivní faktory (náklady, čas, dostupné technologie, technologický rozvoj, apod.)

Osobní údaje

nepatří firmě, organizaci či jakékoliv jiné instituci jako nějaká věc, s níž může nakládat dle libosti

Osobní údaje nejsou komodita

Nemohou být předmětem byznysu bez vědomí subjektu údajů

Tyto instituce mohou být nanejvýš správci těchto údajů. Údaje jsou jim propůjčeny, musejí s nimi nakládat v mezích právních pravidel a předpisů.

„osobními údaji“ -

nejsou údaje o právnické osobě

jsou údaje o činnosti fyzické osoby podnikající (OSVČ)

snaha zařadit údaje o OSVČ jako údaje o právnické osobě a tedy vyjmout je z dopadu GDPR

údaje týkající se zdraví – o.ú. týkající se tělesného nebo duševního zdraví FO, včetně údajů o poskytování zdravotních služeb, které odhalují informace o jejím zdravotním stavu

Osobní údaje týkající se zdravotního stavu
- informace o dané osobě shromážděné v průběhu registrace pro účely poskytování zdravotnických služeb a při poskytování těchto služeb;

- číslo, symbol nebo specifický údaj přiřazený fyzické osobě za účelem její jednoznačné identifikace pro zdravotnické účely;

-informace získané během provádění testů nebo vyšetřování části těla nebo tělesných látek, včetně genetických údajů a biologických vzorků;

Zdravotní údaje (WP29)

Osobní údaje o zdravotním stavu rozdělila do tří skupin:

1. Neodmyslitelná **medicínská data**, …….. v kontextu diagnostika, léčba, anamnéza, …

2. **Data ze sensorů**, která mohou být použita samostatně nebo v kombinaci s jinými daty a vytváření závěrů o aktuálním zdravotním stavu nebo o zdravotních rizicích osoby;

3. **Závěry o zdravotním stavu …….** bez ohledu na to, zda tyto závěry jsou či nejsou přesné, legitimní nebo adekvátní.

Písemné odpovědi uvedené zkoušeným při odborné zkoušce a případné korekturní poznámky zkoušejícího pojící se k těmto odpovědím představují osobní údaje ve smyslu definice

Rozsudek Soudního dvora EU (druhého senátu) ze dne 20. prosince 2017 (žádost o rozhodnutí o předběžné otázce Supreme Court – Irsko) – Peter Nowak v. Data Protection Commissioner

Rozsudek CJEU ze dne 20. 12. 2017 – věc C-434/16

Spor mezi P. Nowakem a Data Protection Commissioner (komisař pro ochranu údajů, Irsko)

odepření přístupu k opraveným odpovědím ze zkoušky z důvodu, že informace obsažené v odpovědích nejsou osobními údaji.

Rozsudek CJEU ze dne 20. 12. 2017 – věc C-434/16 Nowak

GDPR čl. 15:

1. Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak, má právo získat přístup k těmto osobním údajům[…]

3. Správce poskytne kopii zpracovávaných osobních údajů.[…]

4. Právem získat kopii uvedenou v odstavci 3 nesmějí být nepříznivě dotčena práva a svobody jiných osob.

Rozsudek CJEU ze dne 20. 12. 2017 – věc C-434/16 Nowak

Peter Nowak se připravoval na povolání certifikovaného účetního …..úspěšně složil tři zkoušky druhé úrovně organizované Institute of Chartered Accountants of Ireland (Institut certifikovaných účetních Irska, dále jen „CAI“). Neuspěl však ve zkoušce ….. ‚při které měli zkoušení možnost používat studijní materiály („open book exam“).

Po čtvrtém neúspěchu při této zkoušce na podzim 2009 podal P. Nowak nejprve stížnost, kterou zpochybnil výsledek této zkoušky. Poté, co tato stížnost byla v březnu 2010 zamítnuta, podal v květnu 2010 podle článku 4 zákona o ochraně údajů žádost o přístup týkající se všech osobních údajů, které se ho týkají a které má v držení CAI.

Rozsudek CJEU ze dne 20. 12. 2017 – věc C-434/16 Nowak

CAI P. Nowakovi odepřel přístup k dokumentu s jeho odpověďmi na zkušební otázky, a to z důvodu, že uvedený dokument neobsahuje osobní údaje ve smyslu zákona o ochraně údajů.
Komisař pro ochranu údajů uvedl, že „písemné odpovědi na zkušební otázky obecně nejsou brány v potaz pro účely [ochrany údajů][…], neboť takový materiál zpravidla není osobním údajem“ a jeho stížností se nebude dále zabývat.

Podpůrně oblastní soud (Irsko) rozhodl, že žaloba je neopodstatněná, protože odpovědi na zkušební otázky nepředstavují osobní údaj.
High Court (Vrchní soud, Irsko) tento rozsudek potvrdil.

Rozsudek CJEU ze dne 20. 12. 2017 – věc C-434/16 Nowak

Supreme Court (Nejvyšší soud) měl pochybnosti a položil CJEU otázku(y):

Mohou být informace či odpovědi uvedené účastníkem odborné zkoušky osobními údaji ve smyslu směrnice 95/46 (resp. GDPR)?

Rozsudek CJEU ze dne 20. 12. 2017 – věc C-434/16 Nowak

CJEU:
.... aby určitý údaj mohl být kvalifikován jako „osobní údaj“ se nevyžaduje, aby se všechny informace umožňující identifikovat subjekt údajů nacházely v rukách jediné osoby

…. naopak subjekt, který zkoušku organizuje disponuje potřebnými informacemi, které mu umožňují bez obtíží nebo pochybností identifikovat zkoušeného prostřednictvím jeho identifikačního čísla uvedeného na odpovědích na zkušební otázky nebo na první stránce těchto odpovědí, a tak k němu přiřadit jeho odpovědi

Rozsudek CJEU ze dne 20. 12. 2017 – věc C-434/16 Nowak

CJEU:

.... výraz „veškeré informace“ v rámci definice pojmu „osobní údaj“odráží cíl unijního zákonodárce přiznat tomuto pojmu široký význam, přičemž tento pojem se neomezuje na informace, které jsou citlivé nebo patří do soukromé sféry, ale potenciálně zahrnuje všechny druhy informací, a to jak objektivní, tak subjektivní ve formě názoru nebo hodnocení pod podmínkou, že jsou „o“ dotčené osobě.

Informace z důvodu svého obsahu, účelu nebo účinku souvisí s určitou osobou.

Obsah těchto odpovědí odráží úroveň znalostí a schopností uchazeče v dané oblasti, jakož i případně jeho myšlenkové pochody, úsudek a kritické myšlení.

Korekturní poznámky zkoušejícího týkající se odpovědí zkoušeného představují informace, které z důvodu svého obsahu, účelu a účinku souvisí s tímto zkoušeným.

Nová definice: Společní správci

Kde správce určuje

účel, podmínky a prostředky zpracování osobních údajů společně s ostatními,

určí společní správci ve vzájemném ujednání, jakou odpovědnost každý z nich nese za plnění povinností vyplývajících z tohoto nařízení, zejména pokud jde o postupy a mechanismy pro výkon práv subjektu údajů

Ustanovení může být vhodné pro různá uskupení poskytovatelů zdravotní služeb

Ne každý obchodní partner .... je zpracovatel

Mnoho organizací v rámci obav z GDPR zaslalo svým obchodním partnerům „zpracovatelské smlouvy“ !

IT technický servis – není zpracovatel

rávce využije pouze ty zpracovatele, kteří poskytují dostatečné záruky zavedení vhodných technických a organizačních opatření tak, aby zpracování údajů splňovalo požadavky GDPR

… se řídí (písemnou) smlouvou , která jej zavazuje vůči správci. Smlouva stanoví předmět, dobu trvání, povahu a účel zpracování, typ údajů, kategorie s.ú., povinnosti a práva

Anonymizace

Pseudonymizace

Výzkumné soubory

Pseudonymizace je prostředek pro zvýšení ochrany údajů, nikoliv pro vynětí zpracování osobních údajů z působnosti Nařízení (údaje nejsou anonymní!)

Správcům pomůže splnit povinnosti týkající se ochrany údajů

Nevylučuje však provedení dalších opatření k ochraně osobních údajů

Souhlas

Souhlas je jedním z (6) důvodů legitimního zpracování údajů

Souhlas není
ani jediným,
ani nejdůležitějším

důvodem zákonnosti zpracování údajů

*„Trvalým tématem jsou **nadbytečné souhlasy** se zpracováním údajů. V České republice je přesouhlasováno. Úplně zbytečně, protože v mnoha případech je správci vyžadovat ani nesmí. Souhlasy mnohdy správci získávají dosti agresivním nebo zavádějícím způsobem, což je samozřejmě v rozporu s obecným nařízením“* - o oblasti, která je v popředí zájmu veřejnosti.

(ředitel sekce správní mgr. Josef Prokeš na listopadové konferenci „GDPR plus 180 dní“)

Sdělení předsedkyně ÚOOÚ
k vyžadování souhlasu

Na základě poznatků z praxe a řady zveřejněných chybných interpretací se Úřad pro ochranu osobních údajů vrací k tématu vyžadování souhlasu a varuje veřejnost, že vyžadování souhlasu může být v řadě případů nadbytečné a v rozporu s obecným nařízením (GDPR).

(ÚOOÚ, 31. 8. 2018)

Dvě části svobodného souhlasu

- svoboda udělení souhlasu
- svoboda trvání souhlasu

Svoboda udělení: bez jakékoliv formy donucení, nátlaku, fyzického nebo psychického

Svoboda trvání: možnost souhlas kdykoliv odvolat

Na svobodném rozhodnutí subjektu údajů závisí zda souhlas bude udělen a jak dlouho bude souhlas trvat

Odvolání neruší souhlas zpětně, nýbrž od okamžiku odvolání !!

Nařízení

stanovuje vysoký standard pro souhlas

Největší změnou s dopadem na praxi, jsou mechanismy získání souhlasu

Správce musí vytvořit mechanismy a způsoby, které umožní - jasně oddělené a rozlišitelné souhlasy v případech opt-in,
- správně je uchovávat a doložit,
- umožnit subjektu údajů jednoduše jej odvolat

Tyto změny odrážejí zásadu, že souhlas musí být dynamický proces (aktivní) ze strany subjektu údajů a náročnější pro získání

Elektronická forma

… může se například jednat o zaškrtnutí políčka při návštěvě internetové stránky, volbu technického nastavení pro služby informační společnosti nebo jiné prohlášení či jednání, které jasně signalizuje souhlas subjektu údajů s navrhovaným zpracováním jeho osobních údajů

Mlčení, předem zaškrtnutá políčka nebo nečinnost - nemohou být považovány za souhlas

INFORMOVANÝ SOUHLAS PACIENTA SE ZPRACOVÁNÍM OSOBNÍCH ÚDAJŮ V REGISTRU

(jméno a příjmení pacienta), **potvrzuji, že jsem byl/a řádně poučen/a o účelu zpracovávání a o rozsahu zpracovávaných osobních údajů v registru provozovaném SPRÁVCEM, se sídlem**

……

Souhlasím ☐ **Nesouhlasím** ☐

(Vámi zvolené políčko zaškrtněte)

aby moje identifikační údaje a osobní údaje související s poskytováním zdravotní péče mé osobě při onemocnění, byly předány mým poskytovatelem zdravotní péče do registru a dále zpracovávány

Získání „nesouhlasu“

GDPR vyžaduje **souhlas** nikoliv **nesouhlas**

Je nutno odlišit informovaný souhlas

- **s poskytnutím zdravotních služeb**
  (§ 34 zák.č.372/2011 Sb.)
- **se zpracováním osobních údajů (čl. 7 GDPR)**

při poskytování zdravotních služeb je „nesouhlas“ pacienta nutno dokumentovat

při zpracování osobních údajů je „nesouhlas“ zbytečný, matoucí a komplikující úkon !!!

Já, níže podepsaný:
Jméno a příjmení:
Rok narození:
Trvalé bydliště:

Souhlasím se zpracováním osobních údajů

Zpracováni bude probíhat v souladu s příslušnými právními normami o ochraně osobních údajů a s Nařízením Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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).

Poskytování Vašich osobních údajů je zákonným požadavkem a máte jako pacient povinnost je poskytnout, stejně jako zdravotnický pracovník má právo je po Vás požadovat.

Neposkytnutí Vašich osobních údajů bude znamenat, že správce Vám nebude moci poskytnout zdravotní služby, a tím může dojít k poškození Vašeho zdraví či přímému ohrožení života.

Byl/a jsem v souladu s příslušnou legislativou poučen/a o svém právu přístupu k těmto údajům a právu na jejich opravu, či omezení zpracování, pokud zjistím, že jsou tyto údaje nesprávné
Doba zpracováni osobních údajů je dle zákona 5let od poslední návštěvy

V Praze dne …….
……. Podpis

Problémy:

- mlčení subjektu údajů (není souhlasem pro zpracování os. údajů)

- neomezená časová platnost souhlasu (souhlas po celý život)

- nemožnost odvolat souhlas (vzdání se práva)

- vědecké studie v medicíně (kdy je nutný souhlas? má pacient právo neposkytnout souhlas pro studii v důležitém veřejném zájmu?)

Práva subjektů údajů

Práva subjektů údajů

- na přístup k údajům
- na opravu
- na přenositelnost údajů
- vznést námitku
- nebýt předmětem automatizovaného individuálního rozhodování
- být zapomenut a právo na výmaz
- na omezení zpracování

Práva subjektů údajů nejsou absolutními právy - je nutno je posuzovat individuálně a s ohledem na stanovená omezení

Příklad z praxe

Q: *Podle našich právníků má nemocný dle GDPR* ***právo na výmaz*** *a může tedy požadovat výmaz celé své zdravotnické dokumentace*

A: Při uplatnění práva na výmaz (podle čl. 17 GDPR) je nutno vždy posoudit, zda neexistují důvody, kdy tomuto požadavku nelze vyhovět

Uplatnit právo na výmaz zdravotnické dokumentace (resp. vyhovět tomuto uplatnění práva) nelze z několika důvodů:

a) u zdravotnické dokumentace se nejedná o osobní údaje, které by již nebyly potřebné (čl. 17 odst. 1a))

b) (a to především!) zpracování je nezbytné pro splnění právní povinnosti, které se na správce vztahuje.
Vedení zdravotnické dokumentace je právní povinnost poskytovatele zdravotních služeb, která je mu uložena zákonem č. 372/2011 Sb. (§ 53 odst. 1)

DPIA

Posouzení vlivu na ochranu osobních údajů (čl. 35 – Data protection impact assessment)

odst. 4:
Dozorový úřad sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu na ochranu osobních údajů. Dozorový úřad uvedené seznamy předá Evropskému sboru pro ochranu osobních údajů (EDPB)

(EDPB obdržel od dozorových úřadů 260 druhů zpracování)

odst. 5:
Dozorový úřad může rovněž sestavit a zveřejnit seznam druhů operací, u nichž není posouzení vlivu nutné

WP 29 / EDPB

„Pokyny pro posouzení vlivu na ochranu údajů a stanovení, zda „je pravděpodobné, že zpracování údajů bude mít za následek vysoké riziko“ pro účely nařízení 2016/679“

(WP 248 rev.01, duben 2017)

Kritéria pro rozhodnutí správce, zda DPIA provádět či nikoliv by měla být

jasná, konzistentní, pragmatická, srozumitelná

Kritéria by měla být v souladu s pokyny WP29 / EDPB

Jednotlivé dozorové úřady zaslaly své návody, které však vyvolávají obavy, že jejich kritéria nebudou splňovat a nezajistí jednotné cíle DPIA.

Mnohé národní návody se vzájemně liší; obsahují kritéria, která Pokyny WP29/EDPB neuvádějí; různá kritéria jsou kombinována do jednoho kritéria; některé státy uvádějí vysoká rizika zpracování, zatímco jiné státy je neuvádějí; . . .

EDPB Opinion 4/2018

on the draft list of the competent supervisory authority of the Czech Republic regarding the processing operations subject to the requirement of a data protection impact assessment (Article 35.4 GDPR) (Sept. 28, 2018)

https://edpb.europa.eu/our-work-tools/our-documents/opinion-board-art-64/opinion-42018-czech-republic-sas-dpia-list_en

EDPB požaduje, aby ÚOOÚ změnil dokument pokud jde o:

- Odkazy na Pokyny
- Význam velkého rozsahu: zrušení explicitních čísel ve svém seznamu a s odkazem na definice velkého rozsahu uvedené v Pokynech
- Sledování zaměstnanosti: Rada doporučuje, aby byl výslovně uveden odkaz na dvě kritéria v Pokynech
- Mezinárodních předávání: Rada požaduje pozměnit seznam a odstranit odkaz na mezinárodní předávání
- První využití řešení uplatňovaných na území ČR: Rada žádá ÚOOÚ, aby změnil svůj seznam tím, že bod 11 uvede do souladu s pokyny WP29 (č.248) a použije shodnou definici inovační technologie, zejména odstraněním kvalifikace "první žádost"

POVĚŘENEC PRO OCHRANU OSOBNÍCH ÚDAJŮ

články 37 – 39 GDPR

povinné nebo dobrovolné?

pokud povinnost podle GDPR nemají - mohou vytvořit v organizaci funkci obdobnou

Jmenování Pověřence na nepovinném (dobrovolném) základě (čl. 37(4)) však **musí splňovat všechny požadavky a povinnosti** stanovené GDPR

Jiná osoba odpovědná za ooú (dobrovolné) nemůže být na pozici Pověřence pro ochranu údajů (Data Protection Officer) - tento název je vymezen pro GDPR.
Jiná osoba musí mít v pracovní smlouvě jiný název (pracovník pro ochranu soukromí, pracovník pro ochranu údajů apod.)

Nejistota zda jmenovat? - Nutno provést interní analýzu potřeby

Není-li jednoznačně zřejmé, že organizace nemusí jmenovat Pověřence, doporučuje se provedení interní analýzy, zda je nebo není nutné Pověřence jmenovat.

Organizace musí být schopna prokázat, že řádně zohlednila důležité faktory dle čl. 24, odst. 1 - povahu, rozsah, kontext, účel zpracování.

Výsledky interní analýzy musí být organizace schopna předložit dozorovému orgánu. Provedení analýzy je součástí odpovědnosti správce.

GDPR nevyžaduje pro Pověřence žádný certifikát nebo speciální prověření !!!

Výběr a jmenování Pověřence je výlučnou pravomocí správce

Dozorový úřad (DPA) **není zmocněn** vytvořit nebo požadovat další kvalifikační požadavky, standardy či certifikáty pro Pověřence, nebo stanovit další úkoly či odpovědnosti

Certifikáty my měly vzniknout přirozeným vývojem praxe. Důležitou úlohu zde mohou mít univerzity, školy či vzdělávací instituce. DPA by měly tuto aktivitu podpořit

Vztah správce – Pověřenec

Snadná dosažitelnost z každého podniku

dosažitelnost - vztahuje se k úkolům Pověřence pro:

- subjekty údajů,
- orgány dozoru,
- útvary uvnitř organizace (správce a zpracovatele),

- při **poskytování informací a poradenství** o právech a povinnostech souvisejících se zpracováním osobních údajů

K zajištění dostupnosti Pověřence, ať interního nebo externího, je důležité, aby byly k dispozici jeho kontaktní údaje

ÚOOÚ

- doručeno více než 16500 oznámení o jmenování
- přes 200 zpráv o změně pověřence nebo kontaktu na něj
- velký počet z nich ustanoven správci čistě na dobrovolné bázi (tedy že jim to zákon vzhledem k jejich činnosti ani neukládá)
- velký podíl externě působících pověřenců
- pověřenec neví, kdy a kdo jeho jmenování oznámil či na jakém základě byl jmenován
- stížnosti na nedostatečnou dostupnost pověřence působícího pro více správců současně
*- **jeden** pověřenec u 58 správců !! (řada dalších u několika desítek správců)*

https://www.uoou.cz/poznatky%2Duradu%2Dk%2Dnbsp%2Dpouzivani%2Dgdpr/d-32252

Dozorový úřad

Sankce

V dozorové činnosti se Úřadu velmi osvědčily vytýkací dopisy, kterými správce upozorní na chyby

Chyby ale ještě neznamenají a ani vždy automaticky nevedou k udělení pokuty

Co se komunikace ohledně problematického zpracování týče, je vždy potřeba férové, čestné a otevřené jednání

(ředitel sekce správní mgr. Josef Prokeš na listopadové konferenci „GDPR plus 180 dní“)

Facebook fined pre-GDPR maximum of £500,000 by ICO over Cambridge Analytica

Facebook could have been fined £17m or four per cent of global turnover if the breach had occurred under GDPR

British Airways warns that a further 185,000 customers were hit by security breach

GDPR news: Portuguese hospital hit with €400,000 fine for two GDPR violations

Barreiro Hospital had granted nine social workers access to patients' clinical data, while 985 users were registered for doctor-level access despite only 296 physicians working at the hospital. The second fine of €100,000 was imposed for the hospital's inability to ensure the integrity of data security in their system.

Hospital do Barreiro contesta judicialmente coima de 400 M euros de Comissão de Dados

Two separate penalties were imposed after the data watchdog inspected the hospital in early July, with a €300,000 fine applied for failing to respect patient confidentiality, and limiting inappropriate access to patient data. The second fine of €100,000 was imposed for the hospital's inability to ensure the integrity of data security in their system.

The fine represents one of the first publicly-announced GDPR fines issued since the regulations came into force on 25 May this year

Sankce

Vydírání na základě GDPR

„... je pravděpodobné, že nastanou pokusy vydírat podniky vymáháním peněz tím, že se nejprve určí sankce podle GDPR, která by mohla vyplývat z útoku, a pak požadovat výkupné o něco menší než uvedená pokuta.
Což by mohlo vést management k rozhodnutí pokutu zaplatit.“

Návrh zákona o zpracování osobních údajů

- státní orgány malé velikosti (malé obce):
  sankce 5 – 15 tis. Kč

Návrh poslankyně K.: Podle našeho přesvědčení je nutné obce a jimi zřizované organizace chránit před hrozbou vysokých až likvidačních pokut ….

Návrh zákona o zpracování osobních údajů

ÚOOÚ - kompetence k zákonu č. 106/1999 Sb., o svobodném přístupu k informacím (!!)
(schváleno)

Odpovědnost

Odpovědnost správce

za jakékoliv zpracování osobních údajů prováděné správcem nebo jeho jménem

S přihlédnutím
- k povaze, rozsahu, kontextu a účelům zpracování,
- k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob

zavede správce vhodná technická a organizační opatření, aby zajistil a byl schopen doložit, že zpracování je prováděno v souladu s tímto Nařízením

Tato opatření musí být podle potřeby revidována a aktualizována

Pro mnohé subjekty je důraz kladen na problémy související s dodržováním předpisů a na obrovské pokuty za nedodržování předpisů, ale **ve skutečnosti je GDPR rozšířením schopnosti řídit používání osobních dat**

GDPR je také o tom, jak umožnit organizacím vědět, -
- jaké údaje mají,
- zajistit jejich bezpečnost a
- účinně je spravovat,

aby pak mohly identifikovat nové (nejen) obchodní příležitosti

Odpovědnost správce

Povinnost přijmout
- vhodná a účinná opatření k zabezpečení a ochraně osobních údajů

Povinnost doložit, že opatření jsou
- aplikována a
- v souladu s nařízením (zákonem)

Povinnost při tvorbě opatření zohlednit
- povahu, rozsah, kontext a účely zpracování a
- riziko pro práva a svobody fyzických osob


PRIVACY
SECURITY
Soukromí
a
bezpečnost
jdou ruku v ruce
TEACHPRIVACY
Privacy+Security Training
www.teachprivacy.com

Soukromí a bezpečnost jsou související, často se překrývající témata, i když mají některé zásadní rozdíly

Jen proto, že je něco „legální“ ještě neznamená, že je to pozitivní, neškodné

Protiprávnímu použití údajů musí být zabráněno zabezpečením údajů – bezpečnostními opatřeními

Na legitimní, avšak škodlivé využití údajů musí být pohlíženo skrze zachování soukromí

Ot: **Jak vidíte rovnováhu mezi bezpečností a soukromím?**

Preneel: **To není o rovnováze – bez bezpečnosti nemáte soukromí , avšak bez soukromí nejste bezpeční.**

Prof. Bart Preneel

500 million customers affected in massive Marriott hack

The records of 500 million customers of Marriott Hotel Group have been leaked in a huge data breach, with payment details included

Kodexy chování

mají přispět k řádnému uplatňování Nařízení s ohledem na konkrétní povahu různých odvětví, zejména pokud jde o:

a) **spravedlivé a transparentní** zpracování;

b) **oprávněné zájmy**, jež správci v konkrétních situacích sledují;

c) **shromažďování** osobních údajů;

d) **pseudonymizaci** osobních údajů;

e) **informovanost veřejnosti** a subjektů údajů;

f) **výkon práv** subjektů údajů;

g) **informace poskytované dětem** a jejich ochranu a způsob získávání souhlasu nositele rodičovské zodpovědnosti nad dítětem;

h) opatření a postupy k zajištění **bezpečnosti zpracování**;

i) **ohlašování případů porušení zabezpečení** osobních údajů dozorovým úřadům a oznamování těchto případů porušení subjektům údajů;

j) **předávání** osobních údajů **do třetích zemí** nebo mezinárodním organizacím; nebo

k) mimosoudní vyrovnání a jiné **postupy pro řešení sporů** mezi správci a subjekty údajů v souvislosti se zpracováním, aniž by byla dotčena práva subjektů údajů.

Budoucnost

23 let stará směrnice 95/46 (1995)
37 let stará Úmluva 108 (1981)
18 let starý zákon č.101/2000 Sb. (2000)

již nebyly schopny dostatečně čelit novým výzvám digitální společnosti

V dnešním složitém digitálním prostředí dosavadní pravidla neposkytovala

- potřebnou úroveň harmonizace,
- nezbytnou účinnost pro zajištění práva na ochranu osobních údajů

Obecné nařízení 2016/679 (2018)

jak dlouho bude tato legislativa v digitálním věku fungovat ?

jak bude zajištěna ochrana lidských práv v digitálním věku ?

bude možné používání budoucích technologií regulovat legislativou ?

BEUC The European Consumer Organisation

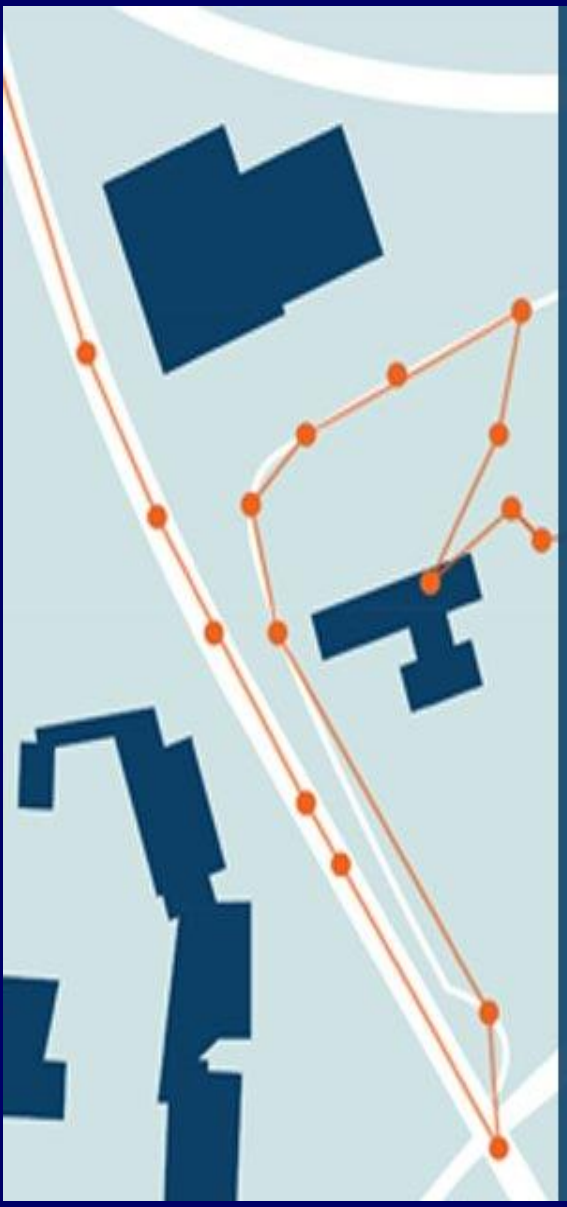
Google bez ohledu na Nařízení Evropské unie pokračuje v zneužívání dat o uživatelích.

Spotřebitelské skupiny v ČR, Řecku, Norsku, Slovinsku a Švédsku podaly stížnost na technologického giganta Google ke svým národním úřadům pro ochranu údajů na základě zprávy norské agentury Forbrukerradet

German court rules in the first GDPR case

No. 1, 25 Oct 2018

Regional Court in Bonn ruled in a case against ICANN (a non-profit organization responsible for global domain name system management).
According to the data minimization principle, registrars should not be required to collect administrative and technical contact information for WHOIS directories.
Penalty 50 000 €



Location data can reveal a lot about people: *religious beliefs* of people visiting a church, *political leanings* because people go to demonstrations and *health conditions* when they regularly visit hospital.

BEUC The European Consumer Organisation

Technologie by neměla diktovat hodnoty a práva

Otázky digitální společnosti mají inženýrské, filozofické, právní a morální důsledky

V dnešním digitálním prostředí dodržovat zákony již nestačí; je nutno posuzovat také **etickou dimenzi** zpracování dat

GDPR
"velký ekosystém ochrany dat": kolektivní úsilí, které se opírá o etické aspekty:

(1) Budoucí orientace na regulaci zpracování údajů a dodržování práv na soukromí a na ochranu údajů
(2) Odpovědnost správců, kteří určují zpracování osobních informací
(3) Ochrana osobních údajů a navrhování produktů a služeb pro zpracování dat
(4) Posílení práv jednotlivců

Respekt k lidské důstojnosti by měl být podstatou nové digitální etiky

Giovanni Butterelli:

Schopnost shromažďovat a využívat velká množství informací a vytváření zisku z této činnosti má dopad na svobodu a soukromí jednotlivce

Obecné nařízení je další kvalitativní krok klasického respektu vůči soukromí jednotlivců

Další vývoj - **směrem k udržitelné etice** v digitalizované společnosti.

„Digitalizace proniká téměř do všech oblastí hospodářství, do našich společenských vztahů, do politiky a vládnutí. Je poháněna především vizí očekávající, že stroje převezmou (dosavadní) lidské rozhodování a odpovědnost za něj“
(říká G.B.)

Giovanni Butterelli:

Technologie je tvořena, používána a řízena převážně člověkem pro jím stanovené účely. Rychle se však blížíme době, kdy tohle všechno bude **svěřeno strojům**.

Etika tak musí právní normy předcházet, prolínat se jejich tvorbou a nastupovat i po jejich schválení. Má vyplňovat prázdná místa tam, kde zákony jsou netečné.
Etika je pro evropské úřady pro ochranu osobních údajů jednou z nejnaléhavějších strategických výzev. Musíme umět porozumět technologii a dokázat vyjádřit sourodý **etický rámec.**

EVROPSKÝ INSPEKTOR OCHRANY ÚDAJŮ

ROZHODNUTÍ
EVROPSKÉHO INSPEKTORA OCHRANY ÚDAJŮ

ze dne 3. prosince 2015,

kterým se zřizuje externí poradní skupina k etickým aspektům ochrany údajů

(„etická poradní skupina“)

Děkuji za pozornost !

Diskuse, dotazy ?