Právo EU v praxi

GDPR a interní audit

19. října 2017 | Praha, ČIIA | Lukáš Lexa & Zdeněk Novotný | Útvar interního auditu České pojišťovny

Co je GDPR

Zpřísnění požadavků na ochranu osobních údajů

- GDPR, neboli **General Data Protection Regulation** je již platné nové Nařízení Evropského Parlamentu a Rady č. 2016/679
- Jedná se o Nařízení EU **upravující nakládání s osobními údaji**
- **Je přímo použitelné**: členské státy jej nemusejí transponovat ani implementovat a jsou za jeho dodržování odpovědné (rozsudky Costa vs. E.N.E.L., Francovich vs. Itálie)
- Účinnosti nabude **25. května 2018**
- Stávající zákon č. 101/2000 Sb. bude do podstatné míry **zrušen či změněn**
- Sankce za nedodržení Nařízení jsou ve výši **až 20 milionů € nebo 4 % celosvětového obratu**
- Zcela nově zavádí povinnost zřídit funkci **pověřence pro ochranu osobních údajů** (Data Protection Officer, dále „DPO“)
- Zavádí nové požadavky na formát osobních údajů: **portabilita a interoperabilita**

Co není GDPR

Revoluce a výlučná oblast IT

- Nejedná se o pouze oblast IT, na kterou nová regulace dopadne
- Nepřináší v zásadě mnoho nového v porovnání se stávající právní úpravou účinnou již 17 let – zák. č. 101/2000 Sb., o ochraně osobních údajů
- Neposkytuje další nástroj pro kverulanty: kultivuje prostředí
- Nedává dozorovému orgánu nové pravomoci, ale navyšuje sankce
- Nezakazuje cloud – ten ale musí být v rámci EHP. Co brexit?

V čem je GDPR problematické

Ústava ČR a LZPS

- Povinnost oznámit dozorovému orgánu únik/zneužití OÚ
- Zásada *nemo tenetur se ipsum accusare*
- Svědčí i právnickým osobám?
- Rozšíření trestní odpovědnosti PO: musí být vyvážené a PO má svědčit i rozšířená ochrana. Zásada legitimního očekávání
- Výše sankce: nesmí být likvidační
- Jak se zákaz diskriminace a princip přiměřenosti promítnou na společném trhu?
- Osobní údaj jako základní lidské právo? Nepostačuje stávající ochrana osobnosti?

Pojmy a instituty spjaté s GDPR

Budete se s nimi setkávat

- Správce vs. zpracovatel
- Subjekt údajů
- Osobní údaj vs. zvláštní kategorie OÚ (dnešní citlivé OÚ)
- Profilace
- Pseudonymizace vs. anonymizace
- „*right to be forgotten*“ (causa Google)
- Portabilita
- Interoperabilita

Správa a zpracování OÚ

Pouze v nezbytném rozsahu

- Existence právního titulu
- Explicitní nepodmíněný graficky oddělený souhlas (nesmí být implicitní nebo konkludentní)
- Zákaz správy zvl. kategorie OÚ, pokud to není nezbytně nutné
- Neúčinnost odvolání souhlasu, pokud správu nařizuje zákon
- Pokud dojde k narušení bezpečnosti, musí být kontaktován subjekt údajů, dozorový úřad a přijata opatření

Náležitosti souhlasu

Pokud jej musíme získat, tak by měl být

- Aktivní – nejlépe podpis nebo zaškrtnutí, formou pop-up okna, vždy opt-in způsobem
- Vyčleněný ze všech obchodních podmínek a hutných textů
- Jasný a srozumitelný – žádné těžké právní texty
- Plný informací – komu se uděluje, proč, na jak dlouho a s jakými právy
- Evidovaný – při kontrole bude potřeba doložit, kdy byl získán a jak vypadal

Jak se dotýká interního auditu?

Potřeba nových kontrol

- Kontrola nezávislosti a efektivity DPO
- Kontrola smluvních vztahů s externími dodavateli a subdodavateli (SLAs)
- Pojišťovny pracují s celou řadu osobních údajů, a to i citlivými (resp. se zvláštní kategorií OÚ)
- Přistupuje k nim velké množství zaměstnanců – potřeba řídit přístupy a uchovávat logy (*corpus delicti*)
- Měly by mít vyhotovené bezpečnostní směrnice (IT bezpečnost a fyzická bezpečnost) a plány pro postup v případě úniku osobních údajů
- S tím souvisí přednastavení komunikačních kanálů – hlášení incidentů, mediální komunikace
- Interní audit neauditue procesy nakládání s OÚ, to je úloha DPO. IA tedy vyhodnocuje jeho činnost
- Přezkoumává ale vnitřní předpisy (příkaz zaměstnavatele)
- Přezkoumává periodicitu školení zaměstnanců – analogie k BOZP

Kdo je DPO?

Pověřenec pro ochranu osobních údajů

- „*DPO*“ podle anglického označení Data Protection Officer
- Musí disponovat odbornými znalostmi v oblasti práva a IT
- Jeho činnost může být outsourcována a může se jednat o právnickou osobu (WP 243 a FAQ)
- Je to funkce, která musí být ustanovena, nelze její plnění svěřit několika stávajícím zaměstnancům zčásti pro oblast IT a zčásti pro oblast práva a roztříštit tak zodpovědnost za výkon funkce
- Jeho postavení a způsob práce jsou analogické k internímu auditu: je organizačně nezávislý

Postavení a úkoly DPO

Články 38 a 39 Nařízení

- je zapojen do veškerých záležitostí souvisejících s OOÚ
- je podporován při plnění svých úkolů
- nedostává žádné pokyny, nemůže být propuštěn ani sankcionován a je přímo podřízený vrcholovým řídícím pracovníkům
- obrací se na něj subjekty údajů
- je vázán tajemstvím
- nesmí být ve střetu zájmů
- poskytuje informace a poradenství správci a jeho zaměstnancům o jejich povinnostech
- monitoruje soulad s Nařízením
- poskytuje poradenství na požádání
- spolupracuje a komunikuje s dozorovým úřadem

Střet zájmů

Zásada Fit & Proper

- Interní i externí DPO nebude nutně vždy ve střetu zájmů, pokud vykonává činnost pro více organizací. ALE: vůči sobě navzájem nejsou v konkurenčním (soutěžním) postavení na volném trhu
- Zaměstnavatel je povinen zkoumat střet zájmů interního i externího DPO (zásada Fit & Proper) v rámci organizace (funkci tedy nemůže vykonávat osoba odpovědná za IT) i mimo ni (monitoring jiných výdělečných aktivit, otázka blízkých osob)
- Uplatnění zásady Fit & Proper je *analogia iuris* ve vztahu k zásadám Solvency II

Odpovědnost

Trestní – za správní delikt – občanskoprávní

- Trest – stačí nedbalost (omisivní)
- Občanskoprávní: za špatnou radu (DPO), za škodu – dle nařízení vlády do 4,5 násobku mzdy/platu, nevztahuje se na úmysl nebo zvlášť hrubé porušení pracovní kázně a na outsourcing – uplatní se skutečná škoda
- § 5 ve spojení s § 2950 – škoda způsobená informací nebo radou

Liberace

Zbavení se objektivní odpovědnosti za správní delikt

- Pachatel vynaložil dostatečné úsilí, které je rozumné po něm požadovat, aby deliktu předešel/zabránil
- Lze preventovat selhání lidského faktoru/úmysl?
- Princip proporcionality: po malé organizaci nelze požadovat totéž, co po market leaderovi
- Nelze se vyvinit z povinností, lze se vyvinit z incidentů tím, že byly vynaloženy přiměřené prostředky
- ALE: dohledový orgán bude hledat benchmark a to zejména u market leadera
- Netýká se trestného činu
- V celém systému je vždy nejslabším článkem člověk

Požadavky na Risk Management (1/4)

Čl. 35 **Posouzení vlivu na ochranu os. údajů** (Data Protection Impact Assessment)

1. Pokud je pravděpodobné, že určitý druh zpracování, zejména **při využití nových technologií**, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek **vysoké riziko pro práva a svobody fyzických osob**, provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

2. Při provádění posouzení vlivu na ochranu osobních údajů si správce vyžádá **posudek pověřence** pro ochranu osobních údajů, byl-li jmenován.

- **Posouzení** provede správce (tedy např. Risk Management, IT Security,…).
- Pověřenec (DPO) dělá **posudek** – tj. nezávisle hodnotí posouzení správce viz čl. 39,c.

Požadavky na Risk Management (2/4)

GDPR požaduje posouzení z pohledu subjektů, ale co **posouzení rizika pro organizaci?**

Posouzení z pohledu organizace by mělo zohledňovat nejen možnou sankci **4 % z obratu**, ale také:

- ✓ náklady na šetření incidentu,
- ✓ náklady na implementaci nařízených nápravných opatření,
- ✓ náklady na informování klientů,
- ✓ (mimo)soudní vyrovnání s klientem,
- ✓ reputační dopad.

Požadavky na Risk Management (3/4)

Související hodnocení a analýzy rizik

- IT Security Risk Assessment apliakcí
- Obecný IT Risk Assessment
- Operational and Compliance Risk Assessment
- Operational Risk Scenario Analysis and Capital Modelling
- Prioritizace GDPR Compliance Gaps Mitigation

Požadavky na Risk Management (4/4)

Čl. 33 **Ohlašování případů porušení zabezpečení osobních údajů dozor. úřadu**

1. Jakékoli porušení zabezpečení osobních údajů správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, **ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob**.

Posouzení vlivu s ohledem na **důvěrnost, integritu, dostupnost** (Čl. 32)

Zejména rizika:

- ✓ neoprávněné zpřístupnění nebo neoprávněný přístup,
- ✓ náhodné nebo protiprávní zničení, ztráta nebo pozměňování předávaných, uložených nebo jinak zpracovávaných údajů.

Požadavky na IT (1/2)

Čl. 32 **Zabezpečení zpracování**

1. 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, provedou **správce a zpracovatel vhodná technická a organizační opatření**, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování (vs. anonymizace),
b) neustálé důvěrnosti, integrity, dostupnosti a odolnost systémů a služeb zpracování,
c) schopnosti obnovit dostupnost osobních údajů a přístup k nim;
d) **procesu pravidelného testování, posuzování a hodnocení účinnosti** zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

3.Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je **dodržování schváleného kodexu chování** uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání **osvědčení** uvedeného v článku 42.

Požadavky na IT (2/2)

Čl. 32 **Zabezpečení zpracování**

3.Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v odstavci 1 tohoto článku, je **dodržování schváleného kodexu chování** uvedeného v článku 40 nebo uplatňování schváleného mechanismu pro vydávání **osvědčení** uvedeného v článku 42.

Osvědčením se **nesnižuje odpovědnost** správce nebo zpracovatele za soulad s tímto nařízením a nejsou jím dotčeny úkoly a pravomoci dozorových úřadů (Čl. 42, odst. 4).

Osvědčení, pečeť a známka dokládajících ochranu údajů dle GDPR

vs.

Certifikace Information Security Management System (ISO 27k)

ISO 27001:2013 - Control A.14.1.4 Privacy and protection of personally identifiable information:

„Privacy and protection of personally identifiable information shall be ensured as required in relevant legislation and regulation where applicable.“

Co mít v případě kontroly

- veškeré informace a souhlasy
- zpracovatelské smlouvy
- záznamy o zpracování (pro koho údaje spravujete, jaké, proč, na základě čeho, na jak dlouho)
- dokumentaci o školení týmu o nakládání s osobními údaji
- interní procesy ke zpracování osobních údajů

…

A v případě incidentu

- záznam z šetření incidentu
- zprávu o nápravných opatřeních

…

Užitečné odkazy

GDPR (CS, EN a další znění)

http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC

Stránky Evropské komise k GDPR

http://ec.europa.eu/justice/newsroom/data-protection/infographic/2017/index_cs.htm

Stránky ÚOOÚ k GDPR

https://www.uoou.cz/gdpr/ds-3938/p1=3938

Dokument Hospodářské komory ČR

https://www.komora.cz/wp-content/uploads/2017/06/PriruckaGDPR_final.pdf

Diskuse

Jak je to u Vás?

- Jak máte organizačně začleněného DPO?
- Je to jeden člověk nebo tým lidí?
- V jaké fázi implementace Nařízení se nacházíte?
- Zapojuje se do procesu interní audit? Jakým způsobem?
- Byla tato oblast v minulosti auditována? Jsou výstupy používány při implementaci?
- Používáte sdílené systémy (CRM)? Využívá jej více entit (skupina)?
- Používáte cloud? Máte jistotu, že data nejsou mimo EHP?
- Máte data storage centralizované?

19. října 2017 | Praha, ČIIA | Lukáš Lexa & Zdeněk Novotný | Útvar interního auditu České pojišťovny