SOUBĚH A KOLIZE ZÁSADY ODPOVĚDNOSTI A DALŠÍCH ZÁSAD ZPRACOVÁNÍ OÚ V PRAKTICKÉ ČINNOSTI SPRÁVCŮ OÚ

Jindřich Kalíšek, advokát

ČPIT 2019 27. 9. 2019

JUDr. Ing. Jindřich Kalíšek, Ph.D. CIPP/E CIPM
Advokát | Mediátor | Pověřenec pro ochranu OÚ
Vinohradská 1511 / 230, Praha 10 – Strašnice
jindrich@kalisek.net (+420) 775 877 046

AUTOR PŘÍSPĚVKU

Jindřich Kalíšek

- Advokát, zapsaný mediátor a pověřenec pro ochranu osobních údajů
- Člen Odborné sekce ČAK pro právo IT a ochranu osobních údajů
- Pověřen pro vybrané společnosti privátní investiční skupiny KKCG
  - Sazka a.s. (největší česká sázková a loterijní společnost / alternativní mobilní operátor)
  - Cestovní kancelář FISCHER, a.s.
  - MND a.s. (dodavatel energií a služeb)
  - DataSpring s.r.o. (poskytovatel hostingu / cloudových služeb)
  - Conectart s.r.o. (telemarketér a provozovatel zákaznických linek)

VÝZKUMNÁ OTÁZKA A TÉMATA PŘÍSPĚVKU

Jaké souběhy a kolize vznikají mezi zásadou odpovědnosti dle čl. 5 odst. 2 nařízení GDPR a dalšími zásadami zpracování, ochrany a zabezpečení osobních údajů normovanými v čl. 25 a 32 nařízení GDPR?

- Systém principů a zásad zpracování, ochrany a zabezpečení osobních údajů (OÚ) podle GDPR
- Souběh a kolize zásad zpracování, ochrany a zabezpečení OÚ
- Praktické dopady kolizí zásad do činnosti správců a zpracovatelů OÚ z perspektivy pověřence pro ochranu OÚ
- Další známé praktické problémy GDPR
  - Správný přístup k GDPR compliance a její optimalizace × Rizikové scénáře
  - Smlouvy o zpracování OÚ
  - Vztahy s kybernetickou a informační bezpečností

SYSTÉM PRINCIPŮ A ZÁSAD ZPRACOVÁNÍ, OCHRANY A ZABEZPEČENÍ OÚ

Základní principy GDPR

- Princip / Zásada odpovědnosti (čl. 74 recitálu + čl. 5 odst. 2 GDPR)
- Princip přístupu založeného na vyhodnocení rizik (čl. 75–78 recitálu + čl. 25 a 32 GDPR)
- Účely zpracování (čl. 39 recitálu + čl. 6 GDPR)

Zásady ochrany OÚ (čl. 78 recitálu + čl. 25 GDPR)

- Zásada záměrné ochrany OÚ (*Privacy by Design*)
- Zásada standardní ochrany OÚ (*Privacy by Default*)

Zásady zpracování OÚ

(čl. 39 recitálu + čl. 5 odst. 1 GDPR)

- Zásada zákonnosti, korektnosti a transparentnosti zpracování
- Zásada účelového omezení shromažďování OÚ
- Zásada minimalizace zpracovávání OÚ
- Zásada přesnosti OÚ
- Zásada omezeného uložení OÚ
- Zásada integrity a důvěrnosti zpracování

Zabezpečení OÚ (čl. 78 recitálu + čl. 32 GDPR)

- Správce a zpracovatel jsou povinni zavést vhodná TOMs, aby zajistili úroveň zabezpečení OÚ odpovídající danému riziku
- Správce a zpracovatel při posuzování požadované úrovně bezpečnosti a výběru a implementaci opatření zohlední *stav techniky, náklady na provedení, povahu, rozsah, kontext a účel zpracování, rizika pro práva a svobody fyzických osob*

NĚKOLIK KRITICKÝCH POZNÁMEK K CÍLŮM A LEGISLATIVNÍ TECHNICE GDPR

- Bezprecedentní kombinace pravé a nepravé právní regulace s organizační a technickou regulací
  - Nepochopení některých konceptů a instrumentů evropským zákonodárcem (čl. 25 a 32 GDPR)
- Legislativní technika neodpovídá zvolenému druhu právního aktu EU
  - Nařízení dle čl. 288 SFEU → obecně závazný a přímo aplikovatelný předpis
  - Právní normy imperfektní, teleologické
  - Obsah deklaratorní, abstraktní až vágní
  - „Nejasná“ osobní působnost normy → nakolik zavazuje subjekty údajů?
- Podstatné otázky právní úpravy ponechány na členských státech
- Rozpor výsledků aplikace legislativy s deklarovanými cíli regulace
  - 27 (28) + 1 právní řád
  - Nízká právní jistota správců a zpracovatelů
  - Frustrace subjektů údajů

SOUBĚHY A KOLIZE ZÁSAD I

- Vnitřní systém zásad zpracování, zabezpečení a ochrany OÚ není vnitřně koherentní → vznikají souběhy a kolize, které mají praktické dopady
  - Zásady, které mají vést k omezení zpracování OÚ
    - > Zásada minimalizace, zásada omezeného uchování OÚ atd.
  - Zásady, které mají vést k nastavení podmínek pro zpracování OÚ
    - > Zásada zákonnosti, zásada účelového omezení shromažďování apod.
- Evropský zákonodárce: Plošné naplňování všech zásad zpracování, zabezpečení a ochrany OÚ adresáty normy (rec. 2, 50, 51) ×
- Praxe: *Všechny zásady jsou si rovné, ale některé jsou si rovnější*
  - Zásada zákonnosti
  - Zásada transparentnosti
  - Zásada účelového omezení shromažďování OÚ
  - Zásada účelového omezení uchování OÚ
  - Zásada minimalizace OÚ + zásada standardní ochrany OÚ

SOUBĚHY A KOLIZE ZÁSAD II

- Souběhy zásad
  - Souběh zásady zákonnosti a korektnosti a zásady účelového omezení shromažďování OÚ
  - Souběh zásady zákonnosti a korektnosti a zásady účelového omezení shromažďování OÚ se zásadou standardní ochrany OÚ a/nebo zásadou minimalizace OÚ
  - Souběh zásady minimalizace OÚ se zásadou omezeného uložení OÚ
  - Souběh zásad standardní a záměrné ochrany OÚ se zásadou integrity a důvěrnosti OÚ
  - Souběh zásady odpovědnosti se zásadou minimalizace OÚ a/nebo zásadami standardní a záměrné ochrany OÚ
  - Další souběhy

SOUBĚHY A KOLIZE ZÁSAD III

- Kolize zásad
  - Kolize zásady odpovědnosti se zásadou minimalizace OÚ a/nebo zásadou omezeného uložení OÚ
  - Kolize zásady odpovědnosti se zásadou integrity a důvěrnosti OÚ a/nebo zásadami ochrany OÚ
  - Kolize zásady zákonnosti a korektnosti se zásadou minimalizace OÚ a/nebo zásadou omezeného uložení OÚ
  - Kolize zásady transparentnosti se zásadou záměrné ochrany OÚ a/nebo zásadou integrity a důvěrnosti OÚ
  - Kolize zásad ochrany OÚ se zásadou omezeného uložení OÚ
  - Vnitřní kolize zásad ochrany OÚ
  - Vnitřní kolize zásady zabezpečení OÚ
  - Aplikační implikace zásady transparentnosti
  - Další kolize

SOUBĚHY A KOLIZE ZÁSAD IV

- Dopady kolizí zásad
  - Primárně snížená právní jistota hlavního adresáta normy (správce, zpracovatele)
    - > Určení, která ze dvou zásad má být zásadou převládající
    - > Určení, do jaké míry konkrétní zásadu naplnit tak, aby nesistovala účinky a výsledky aplikace jiné zásady
    - > Jaké zásady bude považovat za významné DPA
  - Další dopady
    - > Zvýšení nákladů na implementaci a provádění opatření k dosahování shody s GDPR
    - > Zvýšení rizikovosti zpracování OÚ → zvlášť při přeshraničním zpracování
    - > Frustrace vedlejšího adresáta normy (subjektu údajů)

KONKRÉTNÍ SCÉNÁŘE KOLIZE ZÁSAD I

Mohu požádat firmu, se kterou mám uzavřenou smlouvu o poskytování služeb, o smazání mých osobních údajů?

Firma je správcem mých osobních údajů a já nechci, aby je nadále využívala. Smlouvu však s nimi nechci rušit.

Prosím o pomoc. Hledala jsem lupou, ale názory se rozcházely. Webové stránky se SSL certifikátem. Je na nich-na 3 stránkách - formulář na zaslání dotazu, kde se vyplňuje jméno a email a dotaz. V patičce stránek jsou podmínky uchovávání a zpracování údajů. Musí být u každého formuláře políčko na zaškrtnutí souhlasu se zpracování údajů? Děkuji!

Praxe s nadbytečným vyžadováním souhlasů ve školství přetrvává

Největší poradna o GDPR v ČR

Respektujte druhé * Používejte vyhledávání ve skupině * Sdílejte zkušenosti veřejně

Moc prosím, jak je to se zveřejněním například jména nespolehlivého zákazníka třeba na FB. Mám teď zkušenost s paní, která si na zakázku nechala něco vyrobit a teď z ní nemohu dostat peníze. Děkuji

Dobrý den, v rámci home office mzdová účetní odnáší písemné podklady ke mzdám z pracoviště. Dle naší právničky by měl mít zaměstnavatel sepsanou smlouvu s ní jako s fyzickou osobou, že zodpovídá po tu dobu za to, že se podklady nedostanou k jiné osobě (odzizení, omylem nechá v mhd atd.). Prosím nemáte někdo zkušenosti, popř.takovou smlouvu? Děkuji.

Rok s GDPR. Místo jména dítěte zvířátko, marketingové nabídky ale frčí dál

Jmenovky na zvoncích jako problém? GDPR je nekompromisní

KONKRÉTNÍ SCÉNÁŘE KOLIZE ZÁSAD II

Na Ulož.to naleznete firemní hesla, faktury, e-maily i lékařské zprávy

20. března 2019 13:31, aktualizováno 13:56

Analýza více než dvanácti tisíc souborů na serveru Ulož.to odhalila překvapivý problém. Někteří jej využívají pro zálohu nebo sdílení firemních dat a kvůli špatnému nastavení je tak dávají veřejně k dispozici, uvedla společnost Sodat SW, která audit provedla.

Mall.cz dostal za obří únik dat svých uživatelů pokutu 1,5 milionu Kč

28 NÁZORŮ

4. 10. 2018

Loňský únik dat o stovkách tisíc zákazníků Mall.cz ohodnotil Úřad pro ochranu osobních údajů (ÚOOÚ) pokutou 1,5 milionu Kč. „Firma nezabezpečila osobní údaje nejméně 735 tisíc zákazníků," píše ve svém odůvodnění úřad.

Internetový obchod Mall.cz podle ÚOOÚ navíc nedokázal zjistit, jak k úniku došlo.

Skandál ve státním systému. Úřady ve velkém potvrzují pravost falešných dokumentů

Jiří Kubík 26. 2. 2019

- Ulož.to
  - Bezpečnostní audit SODAT
  - 12 tis. souborů → 4,7 tis. smluv a faktur, 10,5 tis. e-mailových příloh, 32 tis. telefonních čísel, 1,3 tis. hesel atd.
- Mall.cz
  - Únik OÚ 736 tis. zákazníků
  - Sankce ÚOOÚ ve výši 1,5 mil. Kč
- Test Ústavu forenzních disciplín na vidimaci falešných dokumentů
  - Notářství, matriky a místa Czech POINT
  - 66 míst po celé republice ☐ vidimováno v 51 případech

KONKRÉTNÍ SCÉNÁŘE KOLIZE ZÁSAD III

- Výzkum Jamese Pavura (University of Oxford, Red Hat Security Conference 2019)
  - 25 % správců zpřístupnila OÚ žadateli, který se identifikoval jako snoubenec/partner subjektu údajů a učinil žádost o přístup k těmto údajům na základě GDPR
  - Předmětem testu desítky společností v US / UK (hotelové řetězce, dopravní společnosti, vzdělávací instituce)
  - Pravidelně poskytnuty informace o kreditní kartě, cestovní informace, přístupové údaje k účtům, US social security number, záznam z rejstříku trestů
- Další mezinárodní průzkumy a statistiky
  - 40 % společností není 10 měsíců po účinnosti GDPR compliant, 60 % z compliant společností je jen v základním stavu compliance, 15 % společností neví, jestli bude compliant v roce 2020 (průzkum BDO z počátku roku 2019)
  - Přes 90 % zaměstnanců neumí rozlišit podvržený e-mail anebo zneužití identity v e-mailové komunikaci (vlastní praktická zkušenost na základě interního bezpečnostního testu)
  - Přes 80 % zaměstnanců důvěřuje e-mailovým přílohám (S3C.cz)
  - Pouze 12 % zaměstnanců bylo obeznámeno s firemními pravidly pro IT bezpečnost (S3C.cz)
  - 97 % organizací nemá vybavení pro obranu proti hrozbám 5. generace (Check Point 2018 Security Report)
  - 77 % organizací nemá Computer Security Incident Response Plan (IBM Cyber Resilience 2018)

KONKRÉTNÍ SCÉNÁŘE KOLIZE ZÁSAD IV

- Šikanózní výkon práv a obcházení právních předpisů výkonem práv subjektu údajů
  - Vynucování „absolutního naplnění“ práv subjektem údajů
- Automatické „vyhovování“ uplatněným právům subjektů údajů
  - Procesní a technická nepřipravenost, zvyšování kyberbezpečnostních rizik
  - Nedostatky v identifikaci a autentifikaci osob
- Nadužívání souhlasů a oprávněných zájmů
- Neposkytování anebo nesprávné poskytování informací o zpracování OÚ
- Přenášení odpovědnosti na zpracovatele OÚ a věcně nemožné smlouvy o zpracování OÚ
- Evidence uplatněných a vyřízených práv subjektů údajů za účelem naplnění zásady odpovědnosti
- Informační systémy s auditní stopou / persistentní storage s omezenou funkční paletou (CRU)
- Nedostatky v obecné kybernetické a informační bezpečnosti správců a zpracovatelů

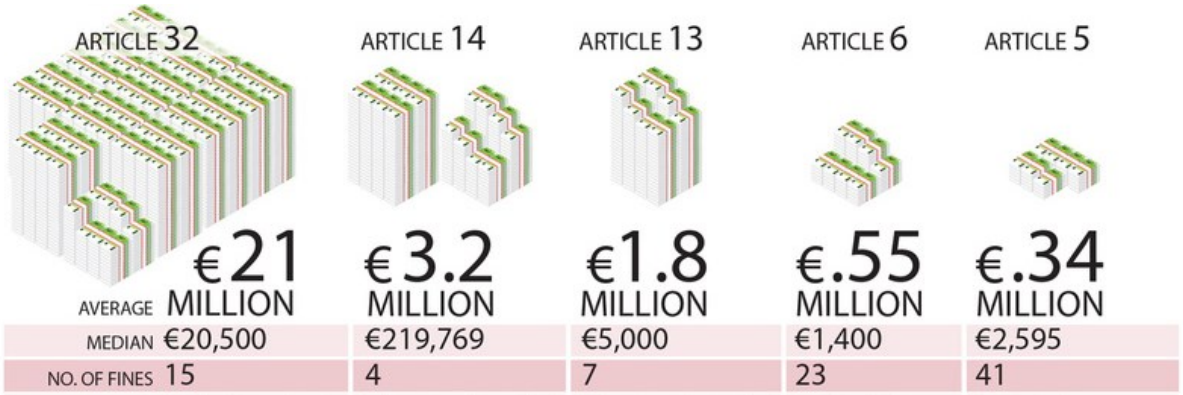
JE POTŘEBA TOMU VĚNOVAT POZORNOST? I

- Analýza Mazar‘s (https://bit.ly/2I3guvL)

Pokuty podle jurisdikce

Pokuty podle průmyslových odvětví

Pokuty podle článků GDPR



JE POTŘEBA TOMU VĚNOVAT POZORNOST? II

- Základní problémy GDPR v roce dva (2019)
  - Adresáti pořád „plavou“ v základních principech a požadavcích GDPR
  - Roste sebevědomí DPA a subjektů údajů
    - > 65 000 hlášení data breaches a 200 000 stížností subjektů OÚ vůči DPA
  - Konec doby hájení ze strany úřadů (ICO v UK, Irsku, CNIL, dánský úřad) a *documentation-only* přístupu
  - První soudní spory a „drakonické“ sankce
  - Chybějící samoregulace (kodexy chování, BCR)

JE POTŘEBA TOMU VĚNOVAT POZORNOST? III

Správný přístup

- Přinejmenším minimální GDPR compliance v rozsahu 7+3
- Rozumná aplikace požadavků s přihlédnutím k prostředí, potřebám a možnostem organizace a jejímu rizikovému profilu (!)
- Integrace do všech procesů a evidencí organizace (i kdyby postupná)
  - Zásady ochrany a zabezpečení osobních údajů (čl. 25 + 32 GDPR)
  - DPIA
  - Change management / Procurement
- Řízené pravidelné zlepšování
  - *Tone from the top*
  - Vzdělávání a zvyšování risk-awareness

Typické rizikové scénáře

Potěmkinova vesnice

Dělo na vrabce

Spekulativní ignorace / Rezignace

Typické aplikační problémy

Chybějící reflexe principů ochrany a zabezpečení osobních údajů

Nedostatečná dokumentace shody

Nedostatečná příprava a implementace prostředí, procesů a opatření

Smlouvy o zpracování osobních údajů a další smluvní vztahy související s nakládáním s informacemi

DESATERO MINIMÁLNÍ GDPR COMPLIANCE (7+3)

- Soubor požadavků, které jsou mandatorní pro každého správce, potažmo zpracovatele
  - Součástí minimální přípravy musí být od počátku vyhodnocení rizik a zohlednění rozsahu, obsahu a kontextu zpracovávaných OÚ

- Aktuální dokumentace naplňování zásad zpracování a ochrany OÚ dle čl. 5, 6, 25 a 32 GDPR → **vyhodnocení významných a koncepčních rizik včetně IT, definice role IT**
- Aktuální záznamy o zpracování OÚ dle čl. 30 GDPR → **úvodní hodnocení rizik, pravidelná aktualizace**
- Naplňování informační povinnosti vůči subjektům údajů dle čl. 12 – 14 GDPR
- Proces naplňování práv subjektů údajů dle čl. 15 – 24 GDPR a vedení jejich evidence → **předcházení bezpečnostním incidentům včetně IT**
- Proces identifikace, vyhodnocení a hlášení bezpečnostních incidentů a vedení jejich evidence → **podrobná analýza rizik – imanentní součást činností IT**
- Revize a renegociace smluv → smlouvy o zpracování OÚ dle čl. 28 GDPR → řízení rizik v downstreamu
- Systém evidence souhlasů subjektů se zpracováním OÚ

- Pravidelné zlepšování, zajišťování awareness a testování prostředí
- Ustavení a zajištění funkce DPO → **přístup, zapojení do řízení, pravidelný risk assessment**
- Provedení posouzení vlivů na zpracování OÚ (DPIA) → **podrobné hodnocení rizik**

Děkuji za Vaši pozornost

Jindřich Kalíšek, advokát

jindrich@kalisek.net
(+ 420) 775 877 046

JUDr. Ing. Jindřich Kalíšek, Ph.D. CIPP/E CIPM
Advokát | Mediátor | Pověřenec pro ochranu OÚ
Vinohradská 1511 / 230, Praha 10 – Strašnice
jindrich@kalisek.net (+420) 775 877 046