Jak se na poslední chvíli připravit na GDPR

Daniel Joksch

15. 5. 2018

Nakladatelství FORUM s.r.o., divize školení a vzdělávání, Střelničná 1861/8a, Praha 8
tel: +420 251 115 579, fax: +420 251 512 422, office@forum-media.cz, www.forum-media.cz

Cíl přednášky

Cíle

- Seznámit se se základními principy a požadavky GPDR
- Seznámit se s nejdůležitějšími kroky implementace požadavků GDPR
  - Záznamy o zpracování osobních údajů
  - Technická a organizační opatření pro zabezpečení osobních údajů
  - Vyřizování požadavků subjektů údajů na aplikaci práv podle GDPR
  - Ohlašování porušení zabezpečení osobních údajů
  - Souhlas se zpracováním osobních údajů
  - Management třetích stran
  - Přenos osobních údajů do třetích zemí
  - Pověřenec pro ochranu osobních údajů

GDPR stručně

Vrátit osobní údaje (OÚ) těm, kterým patří!

- Účinné od 25. 5. 2018 (platné od 24. 5. 2016)
  - Přímo závazné × cca 50 oblastí pro národní úpravu
  - Derogace dosavadní právní úpravy
    (směrnice č. 95/46/ES – DPD)
- Další posilování a precizace práv subjektů OÚ
- Podstatně náročnější administrace zpracování OÚ pro většinu osob a institucí (správci, zpracovatelé)
- Drakonické pokuty
  - Až 2 % celosvětového ročního obratu či 10 mil. €
  - Až 4 % celosvětového ročního obratu či 20 mil. €
    (při zvlášť závažném porušení povinností)

Místní a věcná působnost GDPR

- Čl. 1, 2, 3 a 4 GDPR

- Cíle Nařízení
  - Ochrana OÚ fyzických osob v EU
  - Volný pohyb OÚ v EU

- Všechny formy zpracování
  - Zcela/částečně automatizované
  - Manuální, jsou-li anebo mají-li OÚ být součástí evidence

- Veškeré zpracování OÚ na území EU/EHP, občanů EU a pohyby OÚ v rámci EU/EHP, když:
  - Správce / zpracovatel OÚ sídlí v zemích EU
  - Správce / zpracovatel OÚ nesídlí v zemích EU, ale zpracovává data občanů EU za účelem nabídky zboží, služeb anebo za účelem monitoringu jejich chování na území EU

Vybrané definice GDPR

Osobní údaje

- Čl. 2, 4 a 9 GDPR

Definice OÚ

- *„veškeré informace o identifikované nebo identifikovatelné fyzické osobě,“*
- Subjekt údajů × identifikovatelná osoba

Identifikátory

- *„jméno, identifikační číslo, lokační údaje, síťový identifikátor anebo jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby.“*
- Explicitně i identifikátory spojené s užíváním internetu

Vybrané definice GDPR

Zvláštní kategorie osobních údajů

- Čl. 9 GDPR

- Osobní údaje, které jsou svou povahou obzvláště citlivé z hlediska základních práv a svobod fyzických osob
  - Rasový či etnický původ
  - Genetické údaje
  - Biometrické údaje (za účelem jedinečné identifikace fyzické osoby)
  - Údaje o zdravotním stavu, sexuálním životě nebo sexuální orientaci
  - Politické názory, náboženské vyznání, filozofické přesvědčení
  - Členství v odborech

Vybrané definice GDPR

- Čl. 2 GDPR

- Zpracování
  - Jakákoliv operace nebo soubor operací s OÚ nebo soubory OÚ
  - *Shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení*

- Evidence
  - Jakýkoliv strukturovaný soubor OÚ přístupných podle zvláštních kritérií
  - Centralizovaný × decentralizovaný
  - Rozdělený podle funkčního / zeměpisného hlediska

Vybrané definice GDPR

- Správce
  - Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů
- Zpracovatel
  - Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce
  - Drtivá většina ICT vendorů spadá právě mezi zpracovatele
- Příjemce
  - Fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty
  - Nikoliv orgány veřejné moci v rámci zvláštního šetření v souladu s právem členského státu

Zásady zpracování OÚ dle GDPR

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

Právní tituly zpracování OÚ dle GDPR

- Čl. 6 GDPR

- Splnění smlouvy
- Splnění právní povinnosti
- Ochrana životně důležitých zájmů subjektu údajů anebo jiné fyzické osoby
- Úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci
- Oprávněné zájmy příslušného správce anebo třetí strany

- Souhlas subjektu údajů → vždy zákonné zpracování?

Souhlas se zpracováním OÚ

- Čl. 4 odst. 11, čl. 6 odst. 1 písm. a), čl. 7, 8 a další GDPR
  - Stanovisko WP 29 č. 15/2011 k definici souhlasu (WP 187)
  - ICO (kontrolní orgán VB) – GDPR consent guidance, březen 2017
- Oproti dosavadní právní úpravě zvýšené nároky
  - *„svobodný, konkrétní, informovaný a jednoznačný projev vůle, kterým subjekt údajů dává prohlášením či jiným zjevným potvrzením své svolení ke zpracování svých osobních údajů“*
  - Oddělitelný → Oddělený
  - Aktivní (komisivní) × vyloučen pasivní, mlčky, konkludentní
- Písemný (i elektronický) × Ústní souhlas
  - Pro každý účel a způsob zpracování osobních údajů zvlášť
  - Povinnost unést důkazní břemeno na správci OÚ

Souhlas se zpracováním OÚ

- Jednoznačný projev vůle subjektu OÚ
- Konkrétní a informovaný
  - Musí obsahovat identifikaci správce + zpracovatele + kategorie příjemců
  - Konkrétní účely, způsoby a období zpracování, vymezení OÚ
  - Poučení o právu souhlas odvolat → stejně snadné jako poskytnutí
- Svobodný
  - Poskytnutí služby nebo zboží nesmí být podmíněno udělením souhlasu
  - Nelze, pokud existuje (principiálně) nerovnovážný vztah → pracovněprávní vztahy
- Srozumitelné a snadno přístupné znění, jasný, jednoduchý jazyk
- Zvláštní úprava souhlasu ke zpracování OÚ dítěte při nabídce služeb informační společnosti
  - V ČR zůstane nejspíše zachována věková hranice 13 let → pod ní dává souhlas zákonný zástupce

Souhlas se zpracováním OÚ

Checklist pro souhlasy se zpracováním OÚ

- ICO ← na vodítko WP 29 stále čekáme

- Je souhlas správný právní titul pro zpracování OÚ?
- Je žádost o souhlas jasná, zřetelná a oddělená od ustanovení uživatelských podmínek?
- Žádáme o aktivní opt-in? Nepoužíváme předem zatržená políčka?
- Je text souhlasu jednoduchý a všeobecně srozumitelný?
- Informujeme subjekt, proč chceme OÚ zpracovávat a jak to budeme dělat?
- Žádáme o souhlas položkově?
- Uvádíme jmenovitě naši organizaci a všechny třetí strany?
- Informuje subjekt OÚ, že může svůj souhlas kdykoliv odvolat?
- Zajistili jsme, že souhlas je možné odvolat snadno a rychle?
- Nepodmiňujeme souhlasem poskytnutí naší služby?
- Pokud poskytujeme online služby přímo dětem, žádáme o souhlas pouze v souladu s našimi opatřeními pro ověření věku a získání souhlasu rodičů?

Práva subjektů OÚ

- Čl. 13 a 15 GDPR
  - Rozšíření stávajícího katalogu práv subjektů OÚ → odpovídající povinnosti správce
- Právo na informace o zpracování OÚ
  - Předběžné informace → povinnost nahrazuje registrační povinnost u ÚOOÚ
  - Informování nutno v případě kontroly anebo uplatnění práv subjektů prokázat
  - Průběžné a následné informace → právo na přístup
- Požadavky na sdělení
  - Stručné
  - Transparentní
  - Srozumitelné
  - Snadno přístupné
  - Bezplatné
    - > Lze požadovat přiměřený poplatek zohledňující administrativní náklady spojené s poskytnutím požadovaných informací nebo s učiněním požadovaných úkonů
    - > Jen v případě, je-li žádost podaná subjektem zjevně nedůvodná nebo nepřiměřená, např. při opakování žádosti

Práva subjektů OÚ

- Právo SÚ na přístup k OÚ → právo získat od správce na žádost
  - Potvrzení, zda jsou OÚ subjektu zpracovávány
  - Přístup k těmto OÚ (kopie zpracovávaných osobních údajů)
  - Přístup k určitým informacím
- Poskytované informace
  - Účely zpracování
  - Kategorie dotčených osobních údajů
  - Příjemci nebo kategorie příjemců
  - Doba zpracování
  - Existence práv subjektu (oprava, výmaz, omezení zpracování, námitka, podat stížnost u dozorového orgánu)
  - Zdroj, od kterého byly údaje získány
  - Zda dochází k automatizovanému rozhodování
  - Při předání OÚ do třetí země – vhodné záruky předání
- Požadavky na sdělení shodné jako u práva na informace

Práva subjektů OÚ

- Čl. 17 GDPR – Právo subjektu na vyžádaný výmaz jeho OÚ
  - Nejde o nové právo, již dříve dovozeno judikativou (rozhodnutí *Google*)
- Správce má povinnost bez zbytečného odkladu vymazat OÚ subjektu a nesmí je dále zpracovávat
  - Již nejsou potřebné pro původní účely
  - OÚ shromážděny v souvislosti s nabídkou služeb informační společnosti dítěti
  - Subjekt údajů odvolal svůj souhlas
  - Zpracování OÚ je anebo se v průběhu času stane protiprávním (např. neoprávněné zpracování citlivých údajů, zpracování údajů bez souhlasu subjektu, resp. po jeho odvolání)
  - Právo SÚ žádat o výmaz osobních údajů, které se SÚ týkají
- Správce může žádost odmítnout, pokud je zpracování nezbytné pro
  - Výkon práva na svobodu projevu a informace
  - Splnění právní povinnosti správce podle práva Unie nebo čl. státu
  - Veřejný zájem v oblasti veřejného zdraví
  - Archivaci ve veřejném zájmu, výzkum, statistické účely
  - Určení, výkon nebo obhajobu právních nároků

Práva subjektů OÚ

- Čl. 20 GDPR – Právo na přenos OÚ (*Data portability*)
  - Vodítko WP 29 k právu na přenositelnost (WP 242 rev. 01)
  - Právo subjektu na žádost získat „své“ osobní údaje
  - Právo subjektu předat tyto údaje jinému správci (ideálně přímo od správce k správci)

- Podmínky práva na přenositelnost
  - Zpracování se provádí automatizovaně (forma zpracování)
  - Zpracování na základě předchozího souhlasu nebo k naplnění smlouvy, jejíž stranou je SÚ (důvod zpracování)
  - Osobní údaje se týkají SÚ (rozsah přenášených osobních údajů)
  - Osobní údaje byly poskytnuty SÚ (rozsah přenášených osobních údajů, kategorie dat v závislosti na jejich původu)
  - Právo na přenositelnost se neuplatní na zpracování osobních údajů ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen

Práva subjektů OÚ

- Formát poskytovaných informací
  - Informace se poskytnou v elektronické formě, která se běžně používá, pokud subjekt nepožádá o jiný způsob
- Lhůta k vyřízení
  - Bez zbytečného odkladu do 1 měsíce (možno výjimečně prodloužit)
  - Nevyhovění žádosti: bez zbytečného odkladu do 1 měsíce
- Náhrada nákladů
  - Jedna kopie osobních údajů se poskytne zdarma, za další žádost je možno žádat přiměřenou úhradu nákladů
  - Informace se poskytují bezplatně, ledaže jsou žádosti zjevně nedůvodné nebo nepřiměřené (přiměřený poplatek / odmítnutí žádosti)
- Právem získat kopii nesmějí být nepříznivě dotčena práva jiných osob

---

- Návrh zákona o zpracování osobních údajů
  - § 10 odst. 3 - omezení práva na přístup – je-li to nezbytné a přiměřené pro ochranu práv jiné osoby

Vedení záznamů o činnostech zpracování OÚ

- Čl. 30 a násl. GDPR

- Povinnost vést záznamy o činnostech zpracování
  - Písemné záznamy, dostupné na vyžádání dozorovému úřadu
  - Výjimka pro malé a střední podniky do 250 zaměstnanců
  - Správce je povinen doložit, že:
    - zpracování je prováděno v souladu s nařízením
    - opatření jsou aplikována v souladu s nařízením (zákonem)
    - opatření jsou podle potřeby revidována a aktualizována
    - musí při tvorbě opatření zohlednit:
    - povahu, rozsah, kontext a účely zpracování a
    - různě pravděpodobné a různě závažná rizika pro práva a svobody fyzických osob (*risk-based approach*)

Hlášení data breaches

Bezpečnostní incidenty (*data breaches*) podle GDPR

- Povinnost oznámit příslušnému vnitrostátnímu orgánu (ÚOOÚ) případy porušení zabezpečení osobních údajů **do 72 hodin po datu zjištění**
  - Výjimka z oznamovací povinnosti v případě, kdy narušení bezpečnosti by pravděpodobně nepředstavovalo riziko z hlediska práv a svobod jednotlivce
- Oznámení o narušení bezpečnosti osobních údajů je správce povinen zaslat bez zbytečného odkladu dotčenému jednotlivci
  - Pokud narušení bezpečnosti představuje vysoké riziko pro práva a svobody fyzických osob
- Oznámení určené subjektu údajů se nevyžaduje, jestliže:
  - Správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u údajů dotčených porušením ochrany osobních údajů → šifrování
  - Správce přijal následná opatření, která zajistí, aby již nebylo pravděpodobné, že vznikne vysoké riziko pro práva a svobody subjektů údajů ← Mall.cz
  - By to vyžadovalo nepřiměřené úsilí → veřejné oznámení nebo podobné opatření

Hlášení bezpečnostních incidentů

- Ohlašování případů porušení zabezpečení OÚ dozorovému úřadu
  - Jakékoliv porušení zabezpečení
    - > Výjimka: Nepravděpodobnost rizika pro práva a svobody FO
  - Obsah ohlášení
    - > Popis povahy incidentu, včetně kategorie a počtu dotčených subjektů a OÚ
    - > Jméno a kontaktní údaje pověřence (jiného kontaktního místa)
    - > Popis pravděpodobných důsledků
    - > Popis opatření (přijatých/navržených)
  - Bez zbytečného odkladu / pokud možno do 72 hodin
  - Dokumentace všech incidentů

Hlášení bezpečnostních incidentů

- Oznamování případů porušení zabezpečení OÚ subjektu údajů
  - Porušení s následkem vysokého rizika pro práva a svobody FO × výjimky:
    - OÚ nesrozumitelné (← náležitá technická a organizační opatření)
    - Následná opatření → eliminace vysokého rizika
    - Vyžadovalo by nepřiměřené úsilí → veřejné oznámení / podobné opatření
  - Bez zbytečného odkladu
  - Obsah oznámení
    - Povaha incidentu
    - Informace jako v případě obecného hlášení (body 2-4)

Pověřenec pro ochranu OÚ

- Pověřenec pro ochranu OÚ – Data Protection Officer (DPO)
  - Čl. 37 a násl. GDPR
  - Vodítko WP 29 o pověřencích (WP 243 rev. 01)

- Kdo musí jmenovat pověřence?
  - Každý orgán veřejné moci nebo veřejný subjekt
    - > S výjimkou soudů v rámci své soudní pravomoci
  - Subjekty provádějící v rámci svých hlavních činností:
    - > Rozsáhlé pravidelné a systematické monitorování subjektů OÚ
    - > Rozsáhlé zpracování OÚ zvláštní kategorie a údajů týkajících se rozsudků ve věcech trestních
  - Ten, po němž to bude vyžadovat právo EU anebo právo členského státu EU
    - > V ČR se neočekává zvláštní rozšiřování povinnosti mít DPO

Pověřenec pro ochranu OÚ

- Klíčové úkoly DPO
  - Monitorování zpracování OÚ s cílem zajistit soulad s GDPR
  - Zajišťování provádění práv subjektů údajů
  - Evidenční a reportovací činnost DPO
  - Posuzování vlivu na zpracování OÚ (DPIA, konzultace s dozorovým orgánem)
  - Ohlašování a řešení bezpečnostních incidentů
  - Spolupráce s ÚOOÚ
  - Konzultace a odborná vyjádření uvnitř organizace i navenek
  - Vzdělávání a školení zaměstnanců, případně externích dodavatelů

Pověřenec pro ochranu OÚ

- Postavení DPO v kontextu organizace
  - Odpovídající kompetence
  - Postavení vysokého manažera organizace (B-1, B-2) →
  - Přímý reporting členům nejvyššího vedení organizace

- Zapojení DPO do všech oblastí zpracování OÚ v rámci organizace →
  - Přístup k informacím, databázím, procesům aj. → kontrola předběžná, průběžná a následná
  - Znalostní přístup → DPO zná procesy organizace
  - Organizační přístup → DPO může vstupovat do procesů organizace
  - Technický přístup → DPO má přístup k systémům organizace

- Materiální zdroje
  - Zázemí, personál, podpora → včetně odpovídajícího příjmu
  - Časová disponibilita
  - Pakliže DPO vykonává i jiné úkoly → pevně stanovená časová disponibilita pro výkon činnosti

Ochrana a zabezpečení OÚ

- V GDPR se zásady ochrany OÚ promítají v
  - Přístup založený na riziku (*Risk-based approach*)
  - Zásady zpracování OÚ (čl. 5 odst. 1 GDPR)
  - Záměrná a standardní ochrana OÚ (čl. 25 odst. 1 a 2 GDPR)
  - Požadavky na technická a organizační opatření (čl. 32 GDPR)

- Organizační a technická opatření
  - Ochrana před nějakou hrozbou / snížení zranitelnosti / omezení vlivu nechtěné události / umožnění zotavení organizace
  - Kombinace přístupů, praktik, procedur a mechanismů
    - > **Technická** – opatření na snížení bezpečnostních rizik pomocí prostředků fyzické a technologické povahy
    - > **Organizační** – opatření na snížení bezpečnostních rizik pomocí změn procesů a úpravou dokumentace

Ochrana a zabezpečení OÚ

- Principy návrhu systémové / datové architektury organizace
  - Návrh systémové / datové architektury od počátku tak, že data nepotřebují dodatečnou externí ochranu
  - Organizační a technologická opatření
  - Technologie pro podporu ochrany soukromí (*privacy enhancing technologies – PETs*)

- 7 pravidel ISACA
  - Proaktivní, ne reaktivní ochrana / Prevence před odstraňováním škod
  - Ochrana soukromí jako standardní nastavení
  - Ochrana soukromí součástí návrhu
  - Ochrana údajů přes všechny funkce
  - Zabezpečení end-to-end / Ochrana po celý životní cyklus údaje
  - Transparentnost a otevřenost
  - Respekt a nastavení služby k uživateli

Ochrana a zabezpečení OÚ

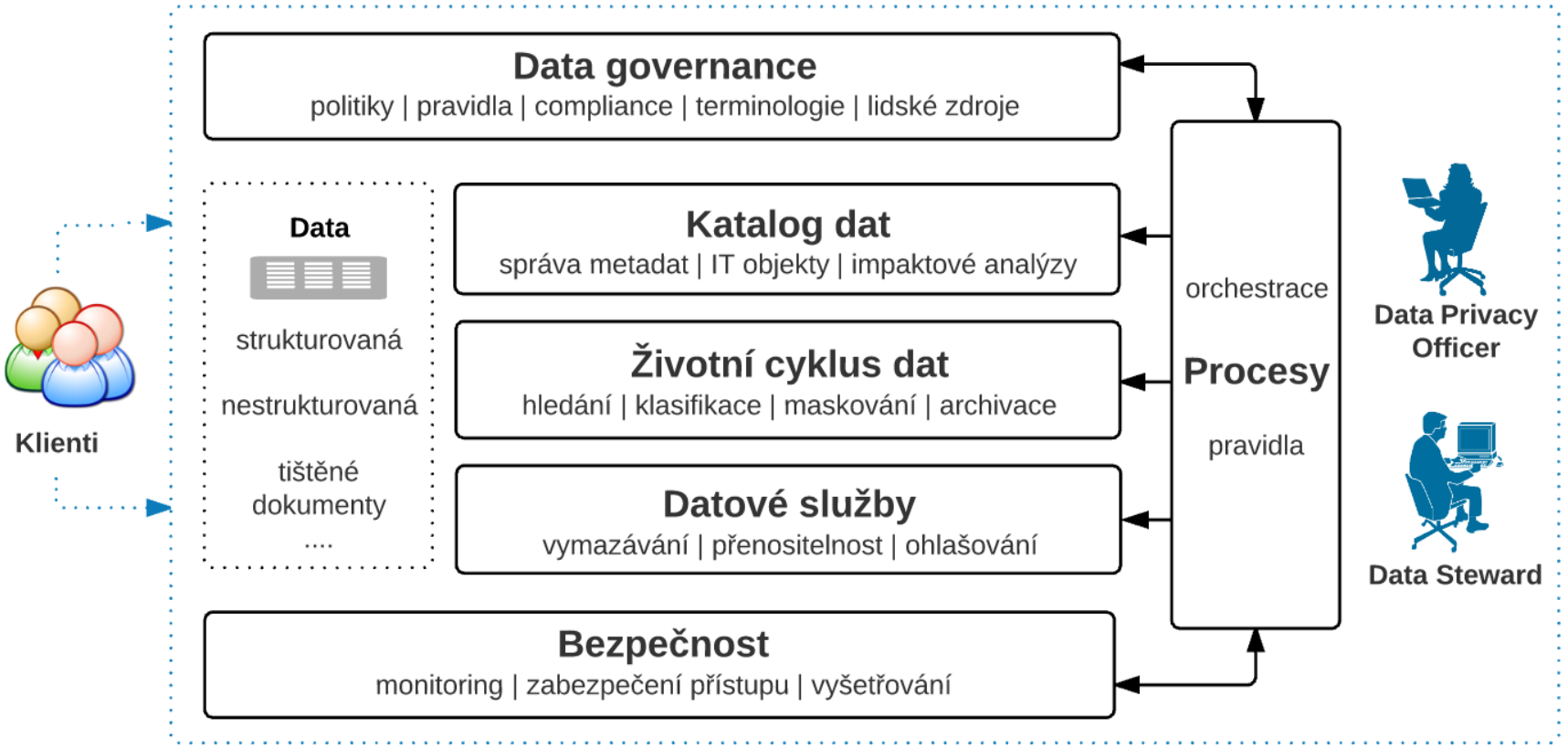
Konkrétní opatření

- Poučení o právech a povinnostech zaměstnanců
- Postup při ukončení pracovního poměru
  - Předání přidělených aktiv, zrušení přístupových práv, poučení o následcích porušení zákonné nebo smluvní povinnosti mlčenlivosti
- Vedení seznamu aktiv a jeho aktualizace, řízení změn
- Kontrola vstupu do objektu a chráněných prostor, správa klíčů
- Přidělování přístupových práv a úrovní přístupu (rolí) oprávněných osob a správa hesel
- Vzájemné zastupování oprávněných osob
- Režim údržby a úklidu chráněných prostor
- Pravidla manipulace s fyzickými nosiči OÚ mimo chráněné prostory
- Pravidla užívání IT prostředků (např. notebooky) mimo chráněné prostory
- Pravidla užívání přenosných datových nosičů mimo chráněné prostory
- Určení postupů likvidace osobních údajů s vymezením související odpovědnosti jednotlivých oprávněných osob

Správa OÚ v organizaci I

- Práva subjektů údajů
  - Právo na informaci
  - Právo na přístup
  - Právo nebýt předmětem automatizovaného rozhodování
  - Právo na aktualizaci
  - Právo pozastavit zpracování
  - Právo na výmaz × možná kolize s právy správce
  - Právo na přenositelnost
- Povinnosti správců a zpracovatelů
  - Povinnost vést záznamy o činnostech zpracování
  - Povinnost zajistit odpovídající zabezpečení OÚ
  - Povinnost ohlašovat bezpečnostní incidenty (*data breaches*)
  - Povinnost provést posouzení vlivu na ochranu OÚ (*DPIA*) a předchozí konzultace
- Procesy na straně organizace
  - Evidence existujícího zpracování OÚ
  - Příprava nového zpracování OÚ
  - Změny schváleného zpracování OÚ
  - Řízení práv subjektů údajů
  - Vztah k ÚOOÚ

Správa OÚ v organizaci II



Přeshraniční zpracování OÚ mimo EU

- Předávání OÚ v rámci EU → svoboda pohybu osobních údajů ×
  - Předávání OÚ do třetích zemí nebo mezinárodním organizacím
- Obecná zásada bezpečnosti zpracování
  - K předání osobních údajů může dojít pouze tehdy, splní-li správce/zpracovatel podmínky nařízení
  - Úprava předání OÚ – cílem zajistit, aby úroveň ochrany FO zaručená GDPR nebyla znehodnocena
- Varianty předávání osobních údajů
  - Předávání založené na rozhodnutí o odpovídající ochraně
  - Předávání založené na vhodných zárukách
  - Předávání založené na výjimkách

Doporučení dalšího postupu

Do účinnosti GDPR zbývá jen 10 dní → **Je třeba začít!**

- Identifikace informačních aktiv a lokalizace OÚ
  - Co? / Kde? / V jakém objemu? / Jak často?
- Popis OÚ, jejich účelů, zákonných titulů a procesů nad OÚ
  - Kdo? / Proč? / Jak? / Kam? / Komu?
- Analýzy rizik a jejich dlouhodobé udržování
  - Úvodní analýza rizik („malá velká DPIA“)
  - Automatizované × Manuální řešení
- Nastavení režimu standardní ochrany OÚ
  - Minimalizace OÚ a revize účelů
  - Purifikace procesů zpracování OÚ
  - Eliminace nepotřebných OÚ (výmaz, pseudonymizace apod.)

Projekt GDPR compliance I

Kombinace tří pohledů přes celou organizaci

- Právní
- Procesní (manažersko-organizační – statický a dynamický)
- Technický (systémový)

Průběh GDPR compliance projektu

- Zhodnocení compliance se stávající právní úpravou (ZOOÚ) → interní audit zpracování OÚ
- Definice/vytvoření systému zpracování OÚ → procesní mapování, reporting
- Check-list kompetencí, povinností a úkolů → Kdo, co, jak?
- Identifikace nových povinností → GDPR, e-Privacy, NIS, PSD2
- Zajištění compliance s GDPR

Projekt GDPR compliance II

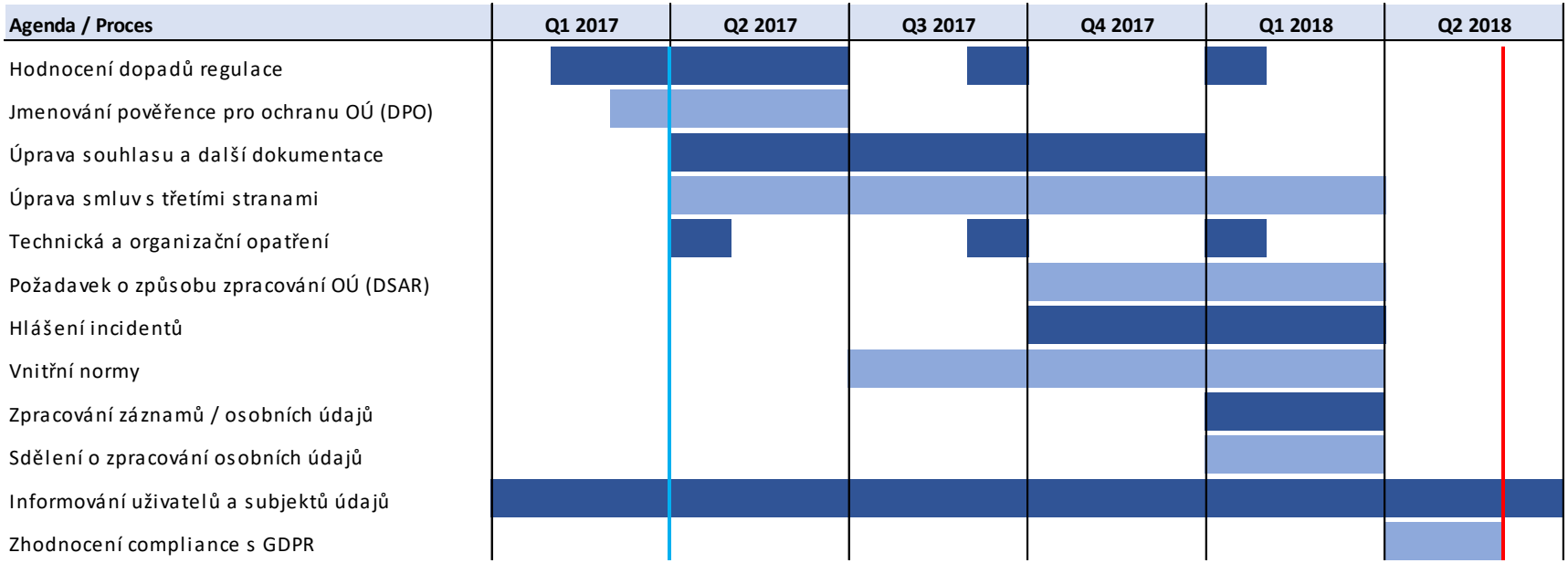
Technická analýza compliance organizace

- Identifikace osobních údajů v datech a procesech
- Technická a organizační opatření
- Posouzení stavu informační bezpečnosti
- Analýza rizik
- Posouzení vlivu na ochranu osobních údajů (DPIA)

Typické problémy

- Nařízené procesy a IS mimo gesci lokálních správců
- Procesy zpracování OÚ nejsou dobře popsány → interní audit
- Není znám rozsah zpracování OÚ a objem databází → interní audit
- Sedimentace IS (legacy IS) → APM

Projekt GDPR compliance III



Posouzení vlivů na zpracování OÚ II

- DPIA je nutné
  - Systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování
    - > Včetně profilování, a na němž se zakládají rozhodnutí, která vyvolávají ve vztahu k FO právní účinky nebo mají na fyzické osoby podobně závažný dopad
  - Rozsáhlé zpracování zvláštních kategorií osobních údajů nebo osobních údajů týkajících se trestních věcí
  - Rozsáhlé systematické monitorování veřejně přístupných prostorů
    - > Např. instalace kamerového systému
- DPIA není nutné
  - Pokud zpracování OÚ nepředstavuje vysoké riziko
  - Pokud již bylo DPIA provedeno pro velmi podobné zpracování
  - Pokud se jedná o zpracování na základě právní povinnosti mající základ v unijním právu nebo právu členského státu EU
  - Pokud je zpracování uvedeno na seznamu zpracování, které nevyžadují DPIA (seznam vypracovaný ÚOOÚ)

Posouzení vlivů na zpracování OÚ III

- Zásady
  - Každé stávající nebo připravované zpracování OÚ
  - Posouzení z hlediska rizik, která představují nebo mohou představovat pro práva a svobody FO

- Jak postupovat?
  - Popis sledovaného druhu zpracování
  - Identifikace přínosů zpracování (nezbytnost a proporcionalita)
  - Identifikace rizikových faktorů zpracování
  - Vyhodnocení stupně rizika
    - > Vysoké riziko? → DPIA
  - Identifikace opatření pro minimalizaci rizik
  - Pokud na základě DPIA nelze nalézt opatření k minimalizaci identifikovaných vysokých rizik →
    - > Zahájit předchozí konzultaci s ÚOOU (čl. 36 GDPR) ×
    - > Nezahajovat posuzované zpracování OÚ

Posouzení vlivů na zpracování OÚ V

- Hodnocení na základě povahy, rozsahu, kontextu a účelů
  - Pohled priority (rizika): vysoké / střední / nízké
  - Pohled severity: kritické / vysoké / střední / malé / nevýznamné
- Faktory pravděpodobně vysokého rizika → DPIA
  - Vyhodnocování osobních aspektů založené na automatizovaném zpracování dat (OÚ)
  - Automatizované rozhodování
  - Rozsáhlé zpracování citlivých osobních údajů
  - Rozsáhlé systematické monitorování veřejných prostor
  - Rozsáhlé zpracování osobních údajů
  - Nové nevyzkoušené technologie
  - Nový způsob zpracování, který ještě nebyl analyzován
  - Další (dle vodítek WP 29)
- Snaha WP 29 vypracovat unijní blacklists / whitelists

Děkuji za pozornost!

© 2018 Daniel Joksch

Tuto konferenci pořádá

Nakladatelství FORUM s.r.o., divize školení a vzdělávání
Střelničná 1861/8a, Praha 8
tel: +420 251 115 576
fax: +420 251 512 422
office@forum-media.cz
www.forum-media.cz