

GDPR krok za krokem

JUDr. Ing. Jindřich Kalíšek

Hotel Troja, Praha, 25. 10. 2017

Přednášející

Jindřich Kalíšek

- Advokát a zapsaný mediátor
- Vedoucí praxe duševního vlastnictví, IT práva a ochrany osobních údajů v PRK Partners
- 7 let praxe v oblasti IP/IT práva a ochrany OÚ
- 5 let praxe v IT/TELCO



Cíle přednášky

- Seznámit se se základními principy a požadavky GDPR
- Seznámit se se specifiky GDPR v otázkách
 - Správy klientských osobních údajů
 - Správy zaměstnaneckých osobních údajů
 - Ochrany, zabezpečení a bezpečnostních incident osobních údajů
 - Pověření na ochranu osobních údajů
- Uvědomit si, že GDPR
 - Je evolucí, nikoliv revolucí na poli ochrany osobních údajů
 - Není žádná věda, ale vyžaduje soustavnou a systematickou přípravu
 - Vyžaduje při dosahování compliance 60 % úsilí v oblasti reengineeringu procesů, zbývajících 40 % se dělí mezi právní a technologické otázky
 - Se rychle blíží →
 - > 7 měsíců na přípravu je jen velmi málo
 - > Pořád se dá udělat *hodně muziky za (relativně) málo peněz*

GDPR: Kroky k dosažení compliance

TO DO

- Základní principy a požadavky GDPR aneb Poznej svého nepřítele!
- Praktické dopady GDPR do organizace
 - Práva subjektů osobních údajů
 - Povinnosti správců/zpracovatelů osobních údajů
 - Klientská data / zaměstnanecké osobní údaje
 - Zabezpečení a ochrana osobních údajů
 - Pověřenec na ochranu osobních údajů
- GDPR compliance projekt
 - Identifikace informačních aktiv a lokalizace osobních údajů – Co? / Kde?
 - Popis osobních údajů, účelů, zákonných titulů a procesů – Kdo? / Proč? / Jak?
 - Analýzy rizik a jejich dlouhodobé udržování – „malá/velká“ DPIA
 - Nastavení zabezpečení a ochrany osobních údajů
- Další otázky

Harmonogram školení



- 09:00 – 10:25 Budoucí legislativní rámec ochrany OÚ v ČR
Zásady zpracování OÚ podle GDPR
Právní tituly / Souhlas se zpracováním OÚ
Dopady GDPR do systému nakládání s OÚ
- (10:25 – 10:30) *Volitelná přestávka*
- 10:30 – 11:30 Katalog práv subjektů
Katalog povinností na straně správců/zpracovatelů OÚ
- 11:30 – 12:15 *Přestávka na oběd*

Harmonogram školení



- 12:15 – 14:00 Vybrané praktické otázky
 - Správa clientských osobních údajů
 - Pracovněprávní problematika a HR praxe
 - Předávání OÚ mezi organizacemiPrincipy ochrany a zabezpečení OÚ podle GDPR
Řízení a hlášení bezpečnostních incidentů

- 14:00 – 14:15 *Přestávka*

- 14:15 – 15:30 Pověřenec na ochranu osobních údajů
Nastavení GDPR compliance projektu
a nezbytné vstupní informace
Úvodní audit stávajících povinností
a stavu zacházení s daty v organizaci
Otázky a odpovědi

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 obrátu či 10 mil. €
 - Až 4 % celosvětového ročního obrátu či 20 mil. € (při zvláště závažném porušení povinností)

Legislativní rámec GDPR



- Nařízení č. 2016/679 – Obecné nařízení o ochraně OÚ (GDPR)
 - Směrnice č. 2016/680 (o ochraně OÚ v trestních věcech)
 - Směrnice č. 2016/681 (PNRD)
 - Derogace směrnice č. 95/46/ES o ochraně OÚ (*Data Protection Directive*)

- Výkladová praxe WP 29
 - Vodítko k právu na přenositelnost údajů (WP 242)
 - Vodítko k pověřenci pro ochranu osobních údajů (WP 243)
 - Vodítko k určení vedoucího dozorového úřadu (WP 244)
 - Vodítko k provádění DPIA (WP 248)
 - Stanovisko k zpracování osobních údajů v zaměstnání (WP 249)
 - Vodítko k hlášení porušení zabezpečení ochrany osobních údajů (WP 250)
 - Vodítko k automatizovanému individ. rozhodování a profilování (WP 251)
 - Průběžná aktualizace

Legislativní rámec GDPR

II

- Obecné právní předpisy
 - Z. č. 89/2012 Sb., občanský zákoník
 - Z. č. 101/2000 Sb., o ochraně osobních údajů (ZOOÚ)
 - Z. č. 40/2009 Sb., trestní zákoník + z. č. 418/2011 Sb., o trestní odpovědnosti PO
 - > § 180 – Neoprávněné nakládání s osobními údaji
- Zvláštní právní předpisy → 1 300 předpisů hovoří o ochraně OÚ
 - Z. č. 262/2006 Sb., zákoník práce + předpisy o zaměstnanosti
 - Z. č. 372/2011 Sb., o zdravotních službách + předpisy o sociální péči
 - Z. č. 499/2004 Sb., o archivnictví a spisové službě
 - Z. č. 480/2004 Sb., o některých službách informační společnosti
 - Z. č. 181/2014 Sb., o kybernetické bezpečnosti
 - Z. č. 284/2009 Sb., o platebním styku + předpisy o finančnictví, pojišťovnictví, bankovníctví a obchodování na finančních trzích
 - Z. č. 280/2009 Sb., daňový řád
 - Z. č. 106/1999 Sb., o svobodném přístupu k informacím
 - Z. č. 256/2013 Sb., katastrální zákon
 - Z. č. 361/2000 Sb., o silničním provozu
- Výkladová praxe ÚOOÚ

Legislativní rámec GDPR

III

Regulátoři a dozorové úřady

- *European Data Protection Board* (EDPB) → náhrada WP 29
- Úřad na ochranu osobních údajů (ÚOOÚ)

Zákon o zpracování osobních údajů a změnový zákon

- Přímá závaznost a aplikační přednost GDPR před ZOOÚ →
- Adaptace GDPR a zčásti implementace směrnici č. 2016/680
 - Zpracování OÚ dle GDPR
 - Zpracování OÚ v trestněprávních věcech
 - Zpracování OÚ při zajišťování obrany a bezpečnosti
 - Postavení a pravomoc ÚOOÚ
- Doprovodný změnový zákon
 - Navazuje na návrh ZZOÚ a implementuje směrnice č. 2016/680 a č. 2016/681
 - Novelizace 19 zákonů
- Plánovaná účinnost k 25. 5. 2018

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

Místní a věcná působnost GDPR

II

– Výluky působnosti GDPR

- Právnícké osoby × ochrana OÚ zaměstnanců
- Zesnulé fyzické osoby a mrtvě narozené děti
- Manuální zpracování nevidovaných OÚ
- Zpracování FO pro výlučně osobní a domácí činnosti
- Zpracování OÚ v oblasti ochrany zákonnosti a bezpečnosti
 - > Výkon činností mimo působnost práva EU
 - > Výkon činností v rámci společné zahraniční a bezpečnostní politiky EU
 - > Prevence, vyšetřování, odhalování a stíhání trestné činnosti
- Anonymní a anonymizované údaje
- (Neidentifikující) údaje pro statistické a výzkumné účely

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

- 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

- 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

Vybrané definice GDPR

V

- Porušení zabezpečení osobních údajů
 - *Data breach*
 - Porušení zabezpečení, které vede k náhodnému anebo protiprávnímu zničení, ztrátě, změně anebo neoprávněnému poskytnutí anebo zpřístupnění přenášených, uložených nebo jinak zpracovávaných OÚ

Zákaz zpracování zvláštní kategorie OÚ

- Čl. 9 GDPR
 - Výjimky
 - Plnění povinností v oblasti pracovního práva, soc. zabezpečení
 - Ochrana životně důležitých zájmů subjektů údajů nebo jiné FO
 - Některá zpracování neziskovými subjekty
 - OÚ zjevně zveřejněné subjektem údajů
 - Obhajoba právních nároků + zpracování soudy
 - Významný veřejný zájem
 - Účely preventivního nebo pracovního lékařství
 - Veřejný zájem v oblasti veřejného zdraví
 - Archivace ve veřejném zájmu
-
- Výslovný souhlas subjektu údajů
 - > Ledaže právo stanoví, že subjekt údajů nemůže souhlas platně udělit

Zásady zpracování OÚ dle GDPR



- Čl. 5 GDPR
 - Možnost omezení aplikace zásad a práv subjektů OÚ za účelem výslovného veřejného zájmu ← čl. 23 GDPR
- Zásada zákonnosti
 - Zpracování OÚ pouze zákonným způsobem, ze zákonných důvodů
 - Čl. 6, 7 GPDR Zákonnost zpracování, podmínky udělení souhlasu
 - Čl. 9 GDPR Zpracování zvláštních kategorií OÚ
- Zásada korektnosti a transparentnosti zpracování
 - Ve vztahu k účelu korektní a transparentní způsoby zpracování
 - Čl. 12 – 14 GDPR

Zásady zpracování OÚ dle GDPR

II

- Zásada účelového omezení shromažďování osobních údajů
 - Určité, výslovně vyjádřené a legitimní účely
 - Zpracování pro účely archivace, vědeckého/statistického výzkumu
 - Další zpracování (čl. 5 GDPR)
- Zásada minimalizace zpracovávání osobních údajů
 - OÚ přiměřené a v relevantním rozsahu
 - OÚ jen v nezbytném rozsahu ve vztahu k účelu
- Zásada přesnosti osobních údajů
 - Včetně aktualizace → zavedení vhodných procesů a opatření

Zásady zpracování OÚ dle GDPR

III

- Zásada omezeného uložení OÚ
 - Ve formě umožňující identifikaci subjektu OÚ jen na dobu nezbytně nutnou pro dané účely zpracování ×
 - Na delší dobu jen pro účely archivace ve veřejném zájmu, výzkumu a statistické účely ← čl. 89 GDPR
- Zásada integrity a důvěrnosti zpracování
 - Náležité zabezpečení OÚ → vhodná technická/organizační opatření
 - Čl. 32 GDPR
- Zásada odpovědnosti
 - Povinnost správce dodržet všechny povinnosti vyplývající ze zásad
 - Povinnost správce dodržení shody prokázat

Právní tituly zpracování OÚ dle GDPR

I

- 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?

Právní tituly zpracování OÚ dle GDPR

II

- Splnění smlouvy
 - Zpracování OÚ potřebných k výkonu smlouvy → vždy zákonné a bez souhlasu
 - Zpracování OÚ během jednání o smlouvě a jejího uzavírání
 - > Předsmluvní odpovědnost
 - > Zásada bezformálnosti
 - Zpracování OÚ po určitou dobu po ukončení jednání o smlouvě
 - > Uzavření smlouvy → čl. 6 odst. 1 písm. b) a c) GDPR
 - > Neuzavření smlouvy → čl. 6 odst. 1 písm. f) a c) GDP

- Ochrana životně důležitých zájmů subjektu údajů anebo jiné fyzické osoby
 - *Kauza ultima ratio* → oběť nehody, která nemůže dát souhlas, třetí osoba v ohrožení života anebo zdraví
 - Humanitární účely, přírodní katastrofy

Právní tituly zpracování OÚ dle GDPR

III

- Splnění právní povinnosti
 - Naplnění právní povinnosti z národního anebo evropského předpisu
 - Explicitní zákonné zmocnění × specifikace konkrétní povinné evidence → není možné uvážení správce, jak povinnost splní
- Úkol prováděný ve veřejném zájmu nebo při výkonu veřejné moci
 - Hlavní právní titul pro zpracování OÚ veřejnou správou →
 - > Využitelný i soukromým subjektem, pokud vykonává veřejnou moc
 - Zpracování OÚ vyplývá z / je nutné pro naplnění úkolu
 - Možnost diskrece na straně správce OÚ

Právní tituly zpracování OÚ dle GDPR

IV

- Oprávněné zájmy příslušného správce anebo třetí strany
 - Velmi flexibilní právní titul
 - > Ochrana práv a chráněných zájmů správce
 - > Správa a ochrana soukromého vlastnictví → kamerové systémy
 - > Vymáhání právních nároků a pohledávek
 - > Monitorování zaměstnanců a pracovníků obecních organizací
 - > Bezpečnost a ochrana zdraví při práci
 - Nezbytné posouzení oprávněnosti zpracování OÚ balančním testem
 - Vyloučený pro plnění úkolů veřejné správy orgány veřejné moci

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

II

- 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) nerovnovážený 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

Dopady GDPR

- Rozšíření informačních povinností správce OÚ vůči subjektu OÚ
- Zavedení povinnosti vést záznamy o činnostech zpracování
 - Výjimka pro malé a střední podniky do 250 zaměstnanců
- Zpřísnění požadavků na poskytovaný souhlas se zpracováním OÚ
- Zavedení institutu posouzení vlivu na ochranu OÚ (*DPIA*)
- Povinnost některých správců a zpracovatelů jmenovat pověřence pro ochranu OÚ (*DPO*)
- Explicitní zakotvení práva na výmaz údajů (*právo být zapomenut*)
- Zavedení práva na přenos údajů k jinému správci (*data portability*)
- Zpřísnění a zpřesnění úpravy obsahu smlouvy o zpracování OÚ
- Přísná úprava ohlašovací povinnosti incidentů v ochraně OÚ
- Významné zvýšení sankcí

(Volitelná) přestávka



GDPR: Kroky k dosažení compliance

TODO



Základní principy a požadavky GDPR aneb Poznej svého nepřítele!

- Praktické dopady GDPR do organizace
 - Práva subjektů osobních údajů
 - Povinnosti správců/zpracovatelů osobních údajů
 - Klientská data / zaměstnanecké osobní údaje
 - Zabezpečení a ochrana osobních údajů
 - Pověřenec na ochranu osobních údajů
- GDPR compliance projekt
 - Identifikace informačních aktiv a lokalizace osobních údajů – Co? / Kde?
 - Popis osobních údajů, účelů, zákonných titulů a procesů – Kdo? / Proč? / Jak?
 - Analýzy rizik a jejich dlouhodobé udržování – „malá/velká“ DPIA
 - Nastavení zabezpečení a ochrany osobních údajů
- Další otázky

Práva subjektů OÚ



- Čl. 13 až 22 GDPR
 - Rozšíření stávajícího katalogu práv subjektů OÚ → odpovídající povinnosti správce

- Čl. 13 a 14 GDPR: 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



- Čl. 15 GDPR: 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

- 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)
 - Právním ziskem 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

Práva subjektů OÚ

IV

- 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



- Lhůty k vyřízení žádosti
 - Bez zbytečného odkladu (→ do 1 měsíce)
 - Nevyhovění žádosti: bez zbytečného odkladu ☞ do 1 měsíce
- Náhrada nákladů
 - Vyřízení žádosti o výmaz nelze zpoplatnit, s výjimkou zjevně nedůvodných nebo nepřiměřených žádostí (např. bezdůvodně se opakujících)
- Povinnost informovat další správce
 - Pokud správce osobní údaje zveřejnil, přijme přiměřené kroky, aby informoval správce, kteří tyto údaje zpracovávají, o žádosti subjektu údajů
- Povinnost informovat subjekt údajů + další zpracování
 - Informace o přijatých opatřeních a pokračujícím zpracovávání určitých údajů (souvisejících s výmazem – oprávněné zájmy správce – důkaz)

- 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

- Výměnný formát → strukturovaný, strojově čitelný, běžně používaný
- Rozsah dat, která se budou muset předávat?
 - Údaje předané subjektem na základě smlouvy anebo souhlasu
 - Údaje získané o subjektu sledováním jeho chování při plnění/užívání služby
 - Na data získaná coby výsledek technické anebo jiné analýzy
- Lhůta k vyřízení
 - Bez zbytečného odkladu → do 1 měsíce (možno výjimečně prodloužit)
 - Nevyhovění žádosti: bez zbytečného odkladu → do 1 měsíce
- Náhrada nákladů
 - Nelze zpoplatnit, s výjimkou zjevně nedůvodných nebo nepřiměřených žádostí (např. bezdůvodně se opakujících)
- Právem na přenositelnost nesmí být dotčena práva a svobody jiných osob
- Právem na přenositelnost není dotčeno právo na výmaz

- Čl. 21 GDPR: Právo subjektu OÚ vznést námitku v případě, že zpracování provádí správce na základě svých oprávněných zájmů
 - Správce má povinnost prokázat, že jeho zájmy převažují nad oprávněnými zájmy namítatele
 - Informační povinnost správce
- Čl. 22 GDPR: Právo subjektu nebýt předmětem automatizovaného individuálního rozhodnutí (včetně profilování)
 - Pakliže se jej významně dotýká
 - Pakliže pro něj má právní účinky

Povinnosti správců a zpracovatelů OÚ

I

- 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*)

Povinnosti správců a zpracovatelů OÚ

II

- Povinnost ohlašovat bezpečnostní incidenty (*data breaches*)
 - Bez zbytečného odkladu, nejpozději do 72 hodin dozorovému orgánu
 - Bez zbytečného odkladu v případě závažného úniku i subjektům OÚ
- Povinnost zajistit odpovídající zabezpečení OÚ (čl. 32 GDPR)
 - Povinnost přijmout vnitřní koncepce a vhodná technická a organizační opatření pro zabezpečení zpracování OÚ
 - Zásady záměrné a standardní ochrany osobních údajů
 - Pseudonymizace, šifrování OÚ
 - Neustálá důvěrnost, integrita, dostupnost a odolnost systémů a služeb
 - Business a data recovery
 - Pravidelné testování, posuzování a hodnocení bezpečnosti opatření

Povinnosti správců a zpracovatelů OÚ

III

- Povinnost provést posouzení vlivu na ochranu OÚ (DPIA) a předchozí konzultace
 - Provádí zásadu odpovědnosti a částečně nahrazuje registrační povinnost
 - Povinnost preemptivně posoudit vliv konkrétních operací při zpracování OÚ, které představují vysoké riziko pro práva a svobody FO
 - > 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 fyzickým osobám právní účinky nebo mají na fyzické osoby podobně závažný dopad
 - > Rozsáhlé zpracování citlivých osobních údajů nebo osobních údajů týkajících se trestních věcí
 - > Rozsáhlé systematické monitorování veřejně přístupných prostorů (typicky instalace kamerového systému)
 - Povinnost předběžné konzultace s dozorovým orgánem
 - > Pokud z DPIA vyjde vysoké riziko a nejsou dostupná opatření k jeho snížení

Povinnosti správců a zpracovatelů OÚ

IV

- Řízení vztahů s ÚOOÚ
 - Povinnost registrace zpracování u ÚOOÚ odpadá → DPIA + předběžné konzultace
 - Stížnosti subjektů OÚ u ÚOOÚ
 - Kontrolní činnost ÚOOÚ → Inspekce
 - Hlášení bezpečnostních incidentů
 - Orgány veřejné moci mají postavení specifických správců OÚ ze zákona
 - > Zásada enumerativnosti veřejnoprávních pretenzí
 - > Obecné zásady spolupráce správních orgánů
 - > Metodické vedení ÚOOÚ a resortních ÚSÚ

Ohlášení 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)

Přestávka



GDPR: Kroky k dosažení compliance

TODO



Základní principy a požadavky GDPR aneb Poznej svého nepřítele!

- Praktické dopady GDPR do organizace
 - ✓ Práva subjektů osobních údajů
 - ✓ Povinnosti správců/zpracovatelů osobních údajů
 - Klientská data / zaměstnanecké osobní údaje
 - Zabezpečení a ochrana osobních údajů
 - Pověřenec na ochranu osobních údajů
- GDPR compliance projekt
 - Identifikace informačních aktiv a lokalizace osobních údajů – Co? / Kde?
 - Popis osobních údajů, účelů, zákonných titulů a procesů – Kdo? / Proč? / Jak?
 - Analýzy rizik a jejich dlouhodobé udržování – „malá/velká“ DPIA
 - Nastavení zabezpečení a ochrany osobních údajů
- Další otázky

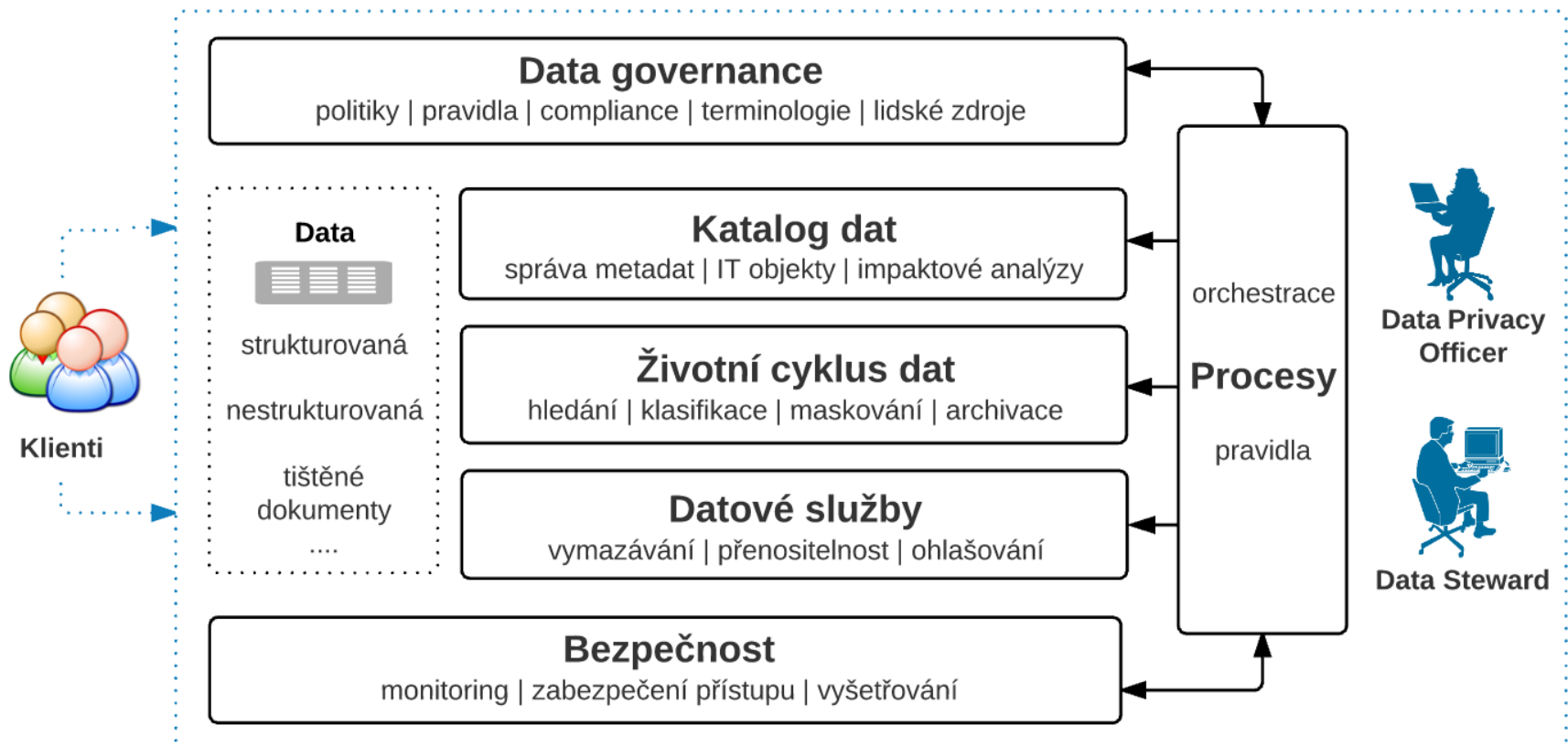
Správa OÚ v organizaci

- 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



Správa klientských OÚ



- GDPR v rámci organizace dopadá na
 - Všechny OÚ
 - > Zákazníci
 - > Zaměstnanci
 - > Dodavatelé / Obchodní partneři × OÚ statutárních orgánů a podnikatelů
 - Celý životní cyklus OÚ
 - > Získání → Zpracování → Aktualizace → Vyřazení

- Jednání o smlouvě se subjektem údajů
 - Oprávněný zájem na zpracování OÚ během jednání o smlouvě a jejího uzavírání
 - > Předšmluvní odpovědnost
 - > Zásada bezformálnosti
 - Oprávněný zájem zpracovávat OÚ po určitou dobu po ukončení jednání o smlouvě
 - > Uzavření smlouvy → čl. 6 odst. 1 písm. b) a c) GDPR
 - > Neuzavření smlouvy → čl. 6 odst. 1 písm. f) a c) GDPR

Správa klientských OÚ



- Správa smlouvy se subjektem údajů
 - Sledování plnění smlouvy ze strany subjektu údajů
 - Komunikace se subjektem údajů, týkající se plnění smlouvy
 - Účetní agenda
 - Vedlejší práva/povinnosti ze smlouvy (odpovědnost za vady, záruky, zajištění, ručení apod.)
- Marketing a související procesy
 - Zpracování OÚ pro marketing a propagační akce → vedle GDPR i zvláštní právní úprava
 - Monitoring chování subjektu údajů při užívání koupeného produktu/služby za účelem marketingu ← právním titulem není smlouva, ale souhlas
 - Přímý marketing spadá pod oprávněné zájmy správce
- Archivace OÚ → Likvidace OÚ

Správa zaměstnaneckých OÚ

I

Dopady GPDR do pracovněprávní praxe

- Posílení odpovědnosti a rozšíření povinností na straně smluvních partnerů zaměstnavatelů
 - Revize zapojení dodavatelů služeb nakládajících s OÚ zaměstnanců
 - > Poskytovatelé HRIS, externí mzdové účtárny, recruitment agencies, agentury práce, smluvní lékař ad.

- Posílení odpovědnosti zaměstnavatelů při přeshraničních transferech OÚ zaměstnanců
 - Zaměstnavatelé musejí být schopni prokázat legitimitu transferů a minimální míru ochrany osobních údajů v zahraničí
 - Při masivních anebo systematických převodech údajů mohou být zaměstnanci v pozici tzv. zranitelných subjektů → DPIA, popř. předchozí konzultace s ÚOOÚ
 - Vyšší význam tzv. závazných podnikových pravidel (*Binding Corporate Rules* – BCR) pro zpracování OÚ v zahraničí
 - > Cloudová uložení
 - > Provoz center sdílených služeb (SSI / CSI)

Správa zaměstnaneckých OÚ



- Omezení významu souhlasu zaměstnanců se zpracováním
 - Základní vedení personálně-mzdové agendy je právní povinností → souhlas pojmově vyloučen
 - V dalších případech ztřené požadavky GDPR
- Rozšiřuje se informační povinnost zaměstnavatele vůči zaměstnancům
 - Zaměstnanci mohou jako subjekty OÚ žádat o široké spektrum informací o tom, jak jsou jejich OÚ zpracovávány → nutná revize dokumentace
- Povinnost mlčenlivosti zaměstnanců správců a zpracovatelů OÚ
 - GDPR výslovnou a jednoznačnou úpravu mlčenlivosti neobsahuje
 - § 15 ZOOÚ stanoví jednoznačnou povinnost (i po skončení zaměstnání) ×
 - > § 12 návrhu ZZOÚ mlčenlivost upravuje jen pro DPO a jemu podřízené osoby

- Zpracování OÚ v rámci personálně-mzdové agendy
 - Základní účel zpracovávání OÚ zaměstnanců
 - Pokrývá i vedlejší zpracování OÚ zaměstnanců, je-li nezbytné pro naplňování pracovněprávních povinností
 - > Práce s životopisy kandidátů během výběrového řízení
 - > Použití fotografie ve spisu či na vstupní průkazce zaměstnance
 - > Evidence práce - docházkové/vstupní systémy
 - > Další povinné databáze/evidence (úrazy, cizinci apod.)
 - > Evidence pro plnění povinností podle ZP/smlouvy (odměňování, benefity, dovolená, překážky v práci, postižení, BOZP, PLS)
 - > Přiměřená kontrola zaměstnanců při použití vybavení zaměstnavatele
 - > Mzdové databáze (odvody, dávky, důchody apod.)
 - > Povinné uchovávání dokumentů/údajů po skončení vztahu

- Další samostatná zpracovávání OÚ zaměstnanců
 - Sběr a zpracování OÚ mimo základní účel zpracování → souhlas
 - > Vedení databáze zájemců o práci
 - > Fotografie zaměstnanců na internetu/intranetu anebo v PR materiálech
 - > Správa HR záležitostí v rámci skupiny jinou (např. mateřskou) společností
 - > Monitoring emailů / sítě
 - > Monitoring GPS služebních vozidel
 - > Kamerový systém s uchováváním záznamu
 - > Nahrávání telefonních hovorů
 - > Whistleblowing Policy
 - > Uchovávání OÚ bývalých zaměstnanců (jiných než povinných)
 - > Databáze zaměstnanců – zákazníků
 - > Nakládání s OÚ rodinných příslušníků pro kontaktování v případě nouze

Monitoring zaměstnanců

Monitoring zaměstnanců – stále aktuální téma

- GDPR může spojovat s permanentním monitoringem nové povinnosti
 - Jmenování pověřence na ochranu OÚ
 - Povinné posouzení vlivu na zpracování OÚ + předběžná konzultace
 - Vodítka WP 243, 248 a 249
- Právní úprava velmi problematická a nestabilizovaná
 - Neexistuje definice monitoringu (ani v ZOOÚ, ani v ZP/ZZ/ZIP) →
 - Není dostatek informací a vodítek jak postupovat (WP 249)
 - Zásadně odlišný přístup ÚOOÚ a inspekce práce
- Obecně jde o sledování zaměstnanců, jejich aktivit a činností
 - Monitoring emailů (včetně DLP a obdobných systémů)
 - Monitoring použití internetu
 - Kamerové systémy
 - Zaznamenávání telefonických hovorů
 - Monitoring pohybu služebních vozidel (GPS) / lokátory pohybu jiného vybavení
 - Monitoring počítače a dalšího vybavení zaměstnance

Ochrana a zabezpečení OÚ



- Čl. 25 GDPR – Záměrná a standardní ochrana OÚ
- Standardní ochrana OÚ (čl. 25 odst. 2 GDPR)
 - Průmět zásady minimalizace → Přijmout vhodná technická a organizační opatření k minimalizaci zpracovávaných OÚ
 - Povinnost standardně zpracovávat jen OÚ
 - > Nezbytně nutné pro specifikovaný účel
 - > V nezbytně nutném rozsahu
 - > Uchovávat po nezbytně dlouhou dobu
 - OÚ nelze volně zpřístupňovat neomezenému počtu osob
- Záměrná ochrana OÚ (čl. 25 odst. 1 GDPR)
 - Účelem provádět zásady ochrany OÚ a začlenit záruky k ochraně práv subjektů
 - Vhodná technická/organizační opatření k ochraně OÚ → čl. 32 GDPR

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

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

III

- 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

Přeshraniční zpracování OÚ v rámci EU

- Přeshraniční zpracování
 - Správce/zpracovatel je usazen ve více než jednom členském státě + zpracování probíhá v souvislosti s činnostmi provozoven ve více než jednom státě EU
 - Zpracování OÚ, které probíhá v souvislosti s činnostmi jediné provozovny správce/zpracovatele v EU, kterým jsou nebo budou podstatně dotčeny subjekty údajů ve více státech
- Dotčený dozorový úřad (DÚ)
 - Správce/zpracovatel usazen na jeho území
 - Subjekty údajů s bydlištěm na jeho území dotčeny zpracováním
 - Byla u něj podána stížnost
- Vedoucí DÚ
 - Orgán nesoucí hlavní odpovědnost za řešení případů přeshraničního zpracování, koordinuje veškerá šetření
 - Určení vedoucího DÚ – v případě přeshraničního zpracování je příslušný DÚ pro hlavní provozovnu správce/zpracovatele (čl. 56 GDPR)

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

Přestávka



GDPR: Kroky k dosažení compliance

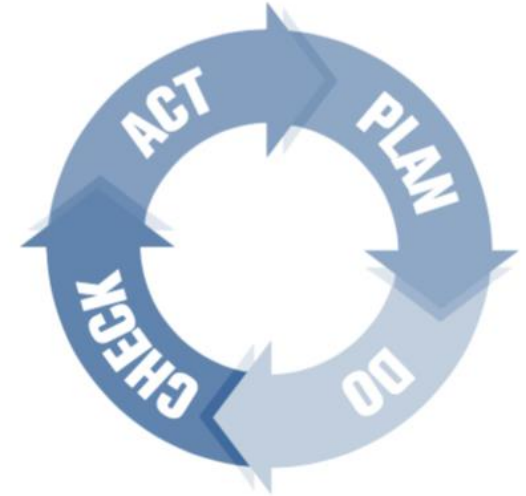
TODO

- ✓ Základní principy a požadavky GDPR aneb Poznej svého nepřítele!
- ✓ Praktické dopady GDPR do organizace
 - ✓ Práva subjektů osobních údajů
 - ✓ Povinnosti správců/zpracovatelů osobních údajů
 - ✓ Klientská data / zaměstnanecké osobní údaje
 - ✓ Zabezpečení a ochrana osobních údajů
 - ✓ Pověřenec na ochranu osobních údajů
- GDPR compliance projekt
 - Identifikace informačních aktiv a lokalizace osobních údajů – Co? / Kde?
 - Popis osobních údajů, účelů, zákonných titulů a procesů – Kdo? / Proč? / Jak?
 - Analýzy rizik a jejich dlouhodobé udržování – „malá/velká“ DPIA
 - Nastavení zabezpečení a ochrany osobních údajů
- Další otázky

Doporučení dalšího postupu

Do účinnosti GDPR zbývá jen 7 měsíců → **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



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



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

Agenda / Proces	Q1 2017	Q2 2017	Q3 2017	Q4 2017	Q1 2018	Q2 2018
Hodnocení dopadů regulace	■	■	■		■	
Jmenování pověřence pro ochranu OÚ (DPO)	■	■				
Úprava souhlasu a další dokumentace		■	■	■		
Úprava smluv s třetími stranami		■	■	■	■	
Technická a organizační opatření		■		■	■	
Požadavek o způsobu zpracování OÚ (DSAR)				■	■	
Hlášení incidentů				■	■	
Vnitřní normy			■	■	■	
Zpracování záznamů / osobních údajů					■	
Sdělení o zpracování osobních údajů					■	
Informování uživatelů a subjektů údajů	■	■	■	■	■	■
Zhodnocení compliance s GDPR						■

Posouzení vlivů na zpracování OÚ

I

- Čl. 35 – 36 GDPR
 - Recitály: 84, 89 – 95
 - Vodítko WP 29 (WP 248)
 - Provádí zásadu odpovědnosti a částečně nahrazuje registrační povinnost
- Povinnost provést posouzení vlivu na ochranu OÚ (*DPIA*)
 - Každé stávající nebo připravované zpracování OÚ → doporučeno i pro současné operace
 - Posouzení vlivu konkrétních operací při zpracování OÚ, které představují nebo mohou představovat vysoké riziko pro práva a svobody FO
 - Pokud je identifikováno vysoké riziko, které nelze eliminovat →
- Povinnost předchozí konzultace s dozorovým úřadem

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 ÚOOÚ (čl. 36 GDPR) ×
 - > Nezahajovat posuzované zpracování OÚ

- Vyhodnocení rizikových faktorů
 - Náhodné nebo protiprávní zničení, ztráta, pozměňování,
 - Neoprávněné zpřístupnění předávaných uložených nebo jinak zpracovávaných osobních údajů nebo neoprávněný přístup k nim
 - Diskriminace, krádež dat, zneužití identity, finanční ztráta, poškození pověsti, ztráta důvěrnosti informací, neoprávněné zrušení pseudonymizace
 - Jakékoliv jiné významné hospodářské nebo společenské znevýhodnění, kdy by subjekty údajů mohly být zbaveny svých práv a svobod nebo možnosti kontrolovat své osobní údaje
 - Zpracování údajů o rasovém či etnickém původu, politických názorech, náboženském vyznání, filozofickém přesvědčení, členství v odborech
 - Zpracování genetických údajů, údajů o zdravotním stavu, sexuálním životě nebo odsouzení v trestních věcech
 - Vyhodnocování osobních aspektů pro vytváření osobních profilů (odhady pracovních výsledků, ekonomické situace, zdravotního stavu, osobních preferencí nebo zájmů, spolehlivosti, chování, místa pobytu a pohybu)
 - Zpracování osobních údajů zranitelných osob (dětí)
 - Zpracování velkého objemu osobních údajů nebo dotýkající se velkého počtu subjektů údajů

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

Posouzení vlivů na zpracování OÚ

V

- V jaký okamžik provést DPIA?
 - Před započítím zpracování × V případě identifikace vysokých rizik
- Osoby zapojené do procesu DPIA
 - Vždy je odpovědný správce (provedením může být pověřen někdo jiný)
 - Vyžádání posudku od DPO (pokud byl jmenován)
 - Stanovisko subjektu údajů nebo jejich zástupců (ve vhodných případech)
- DPIA obsahuje alespoň
 - Popis zamýšlených operací zpracování a účely
 - Posouzení nezbytnosti a přiměřenosti operací zpracování z hlediska účelu
 - Posouzení rizik pro práva a svobody subjektů údajů
 - Plánovaná opatření k řešení těchto rizik (záruky, bezpečnostní opatření, mechanismy k zajištění ochrany a doložení souladu s GDPR)
 - Zohlednění dodržování kodexů chování
- Přezkum s cílem posoudit, zda je zpracování prováděno v souladu s DPIA
 - Při změně rizika – průběžně

Odpovědnost za porušení ochrany OÚ

I

- Čl. 5 odst. 2, 24, 82 GDPR
- Zásada odpovědnosti
 - Povinnost zajistit soulad s GDPR
 - Povinnost být schopen tento soulad aktivně prokázat
- Odpovědnost správce
 - Objektivní (i bez zavinění)
 - Správní / soudní / mimosoudní
 - Soukromoprávní (Právo na ochranu / Právo na náhradu újmy) × Veřejnoprávní (Správní / Trestní)
- Odpovědnost zpracovatele
 - Poruší povinnost, kterou GDPR ukládá přímo jemu
 - Jedná nad rámec zákonných pokynů správce nebo v rozporu s nimi
- Odpovědnost pověřence (DPO)
 - Za soulad s GDPR není odpovědný → možný nárok na náhradu škody

Odpovědnost za porušení ochrany OÚ

II

- Trestný čin „*Neoprávněné nakládání s osobními údaji*“ (§ 180 TZ)
 - Odst. 1 – OÚ shromážděné v souvislosti s výkonem veřejné moci
 - Odst. 2 – porušení státem uložené nebo uznané povinnosti mlčenlivosti

- Další trestné činy
 - Porušení tajemství dopravovaných zpráv (§ 182 TZ)
 - Neoprávněný přístup k počítačovému systému a nosiči informací (§ 230 TZ)
 - Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat (§ 231 TZ)
 - Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti (§ 232 TZ)
 - Jednočinný / vícečinný souběh

- Trestní odpovědnost právnických osob
 - Vyloučena trestní odpovědnost ČR a územně samosprávných celků při výkonu veřejné moci

Odpovědnost za porušení ochrany OÚ

III

- Čl. 83 – 84 GDPR
 - Podmínky pro ukládání správních pokut

- Maximální výše správních pokut
 - Až do výše 10 mil. EUR nebo až 2 % celosvětového ročního obratu
 - Až do výše 20 mil. EUR nebo až 4 % celosvětového ročního obratu

- Novela zákona o inspekci práce
 - § 11a - Přestupky na úseku ochrany soukromí a osobních práv zaměstnanců

- Návrh zákona o zpracování osobních údajů
 - Přestupek porušení zákazu zveřejnění OÚ stanovený jiným právním předpisem
 - Limitace výše pokuty orgánům veřejné moci a veřejnoprávním subjektům – 10 mil. Kč

Q & A

Děkuji za pozornost!

© 2017 Jindřich Kalíšek

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