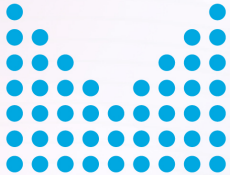


MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Evropská nařízení eIDAS a GDPR v souvislostech

Ing.Robert Piffl

Poradce náměstka ministra vnitra pro ICT

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Poznámka k prezentaci

- *Prezentace byla zpracována výhradně pro potřeby osobní prezentace autora při současném slovním výkladu pro konferenci GDPR a jeho implementace do Krajského úřadu dne 2.10.2017*
- *Bez předchozího svolení autora není možné prezentaci, ani její část využít pro jiný, než výše uvedený účel. Prezentace cituje nikoliv doslovně, ale v odpovídajícím kontextu*
- *Pro zjednodušení problematiky jsou vybírány příklady, splňující určité podmínky, nelze tedy jakkoliv vyvozovat, že by níže uvedené platilo vždy a ve všech kombinacích různých životních situací elektronických dokumentů*
- *Prezentace obsahuje větší množství "slides" jako podkladový materiál pro následné studium účastníkům akce uvedené v prvním odstavci. Ne všechny „slides" budou proto komentovány.*
- *Prezentace zohledňuje stav k 1.10.2017*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ÚVOD

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Nařízení a zákony

- Nová Evropská legislativa
  - existující nařízení eIDAS a GDPR
  - připravované nařízení „jednotná digitální brána pro poskytování informací, postupů, asistenčních služeb a služeb pro řešení problémů“
- Nová národní legislativa
  - právní předpisy související s novými eOP s čipem
  - právní předpisy související s nařízením eIDAS a GDPR
    - Zákon „o službách vytvářejících důvěru“ + zákon „o elektronické identifikaci“
    - Zákon o ochraně osobních údajů – nový

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Legislativa = podmínky pro cíle

- Nová nařízení EU a předpisy na národní úrovni
  - vytváří základní a jednotné podmínky pro dosažení efektivnějšího fungování zejména e-governmentu v EU
  - akcelerátor a příležitost na rozvoj digitálních služeb pro občany
  - efektivní využití nových nástrojů musí vést ke snížení nákladů na ISVS a ne naopak – důslednost kontroly efektivity IT
  - GDPR s ohledem na změnu přístupu k ochraně osobních údajů zajistí bezpečnější IT systémy = zvýšení důvěry občanů k jejich využívání
  - nutno zapracovat na vzdělávání a zvýšení počítačové gramotnosti všech vrstev obyvatelstva

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Přehled vybraných právních předpisů, aneb vymezujeme hřiště

PRÁVNÍ PŘEDPISY

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Aktuální situace v ČR & eIDAS

- Nařízení č. 910/2014 *„**o elektronické identifikaci** a **službách vytvářejících důvěru pro elektronické transakce** na vnitřním trhu a o zrušení směrnice 1999/93/ES“ (dále jen „eIDAS“)*

- K Evropskému nařízení připravilo Ministerstvo vnitra dva základní zastřešující zákony:
  - Zákona o službách vytvářejících důvěru pro elektronické transakce ✓
  - Návrh zákona o elektronické identifikaci ✓

- Výsledný stav je **nařízení a dva vnitrostátní „zastřešující“ právní předpisy** pro oblast nařízení eIDAS

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Jednotná digitální brána EU

- Návrh NAŘÍZENÍ EVROPSKÉHO PARLAMENTU A RADY, kterým se zřizuje jednotná digitální brána pro poskytování informací, postupů, asistenčních služeb a služeb pro řešení problémů z 2.5.2017
  - pravidla pro zřízení a provoz jednotné digitální brány
  - zásada „pouze jednou“
  - pravidla pro hlášení překážek na vnitřním trhu
  - předpoklad – 2 roky adaptační lhůta
  - on-line řešení základních životních situací

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Jednotná digitální brána EU

- Brána poskytuje přístup k informacím o:
  - právech, povinnostech, pravidlech a postupech
  - asistenčních službách a službách pro řešení problémů a odkazům na tyto služby
- Společné uživatelské rozhraní musí být dostupné ve všech úředních jazycích EU
- Požadavky na on-line postupy
- Úložiště odkazů
- Zpětná vazba – tlak na rozvoj e-governmentu v členských státech

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Aktuální situace v ČR & GDPR

- ***Nařízení Evropského parlamentu a Rady (EU) 2016/679*** *ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (**obecné nařízení o ochraně osobních údajů**)*

- K Evropskému nařízení připravilo Ministerstvo vnitra návrh na nového zákona o ochraně osobních údajů – probíhá vnější připomínkové řízení

- Výsledný stav bude **nařízení** a nový zákon místo č. 101/2000 Sb., nařízení má účinnost od **25.5.2018**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ÚOOÚ - web

- Na webu ÚOOÚ je sekce „Obecné nařízení EU (GDPR)
  - cesta: Titulní stránka > Základní odkazy > Obecné nařízení EU (GDPR)
- Dokumenty přeložené pracovní skupiny WP29
  - vodítka k právu na přenositelnost údajů
  - vodítka k funkci pověřence pro ochranu osobních údajů
  - vodítka pro určení vedoucího dozorového úřadu
- Dokument v angličtině pracovní skupiny WP29
  - vodítka k posouzení vlivu na ochranu osobních údajů

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ÚOOÚ - web

- K nařízení užitečné dokumenty
  - rejstřík k obecnému nařízení na ochranu osobních údajů
  - převodní tabulka: zákon na ochranu osobních údajů x obecné nařízení na ochranu osobních údajů
- Obecné nařízení o ochraně osobních údajů v otázkách a odpovědích
- Odkaz na web Evropské komise
  - European Commission-Justice and Consumers>Newsroom>Data protection
- Stanovisko WP29 k návrhu nařízení ePrivacy

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Nařízení a národní právo

- Podle článku 288 Smlouvy o fungování Evropské unie - nařízení jsou přímo použitelná v zemích EU. Soudní dvůr upřesňuje v rozsudku ze dne 14. prosince 1971 ve věci Politi, že se jedná o **úplný přímý účinek**

- Zásada přímého účinku umožňuje jednotlivcům bezprostředně se dovolávat evropských opatření před národním nebo evropským soudem

- **!!! Nařízení mají přednost před vnitrostátními právními předpisy !!!**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Zákon o službách

- Zákon č.297/2016, o službách vytvářejících důvěru pro elektronické transakce
- Zákon č.298/2016, kterým se mění některé zákony v souvislosti s přijetím zákona o službách vytvářejících důvěru pro elektronické transakce, zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, a zákon č. 121/2000 Sb., o právu autorském, o právech o službách vytvářejících důvěru pro elektronické transakce souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů
- oba předpisy **účinnost od 19.9.2016** – konec přechodné lhůty pro podepisování a pečetění „nekvalifikovanými“ 19.9.2018

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Podepisování dle 297/2016 Sb.

Vrchnost

§ 5

K podepisování elektronickým podpisem lze použít **pouze kvalifikovaný elektronický podpis**, podepisuje-li elektronický dokument, kterým právně jedná,

a) stát, územní samosprávný celek, právnická osoba zřízená zákonem nebo právnická osoba zřízená nebo založená státem, územním samosprávným celkem nebo právnickou osobou zřízenou zákonem (dále jen „veřejnoprávní podepisující"), nebo

b) osoba neuvedená v písmenu a) při výkonu své působnosti

K vrchnosti

§6

(1) K podepisování elektronickým podpisem lze použít pouze **uznávaný elektronický podpis**, podepisuje-li se elektronický dokument, kterým se právně jedná vůči veřejnoprávnímu podepisujícímu nebo jiné osobě v souvislosti s výkonem jejich působnosti

(2) Uznávaným elektronickým podpisem se rozumí **zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis nebo kvalifikovaný elektronický podpis**.

Neupraveno

§7

K podepisování elektronickým podpisem lze použít **zaručený elektronický podpis, uznávaný elektronický podpis, případně jiný typ elektronického podpisu,** podepisuje-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 5 nebo § 6 odst. 1.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pečetění dle 297/2016 Sb.

§ 8

- Nestanoví-li jiný právní předpis jako náležitost právního jednání obsaženého v dokumentu podpis nebo tato náležitost nevyplývá z povahy právního jednání, **veřejnoprávní podepisující a jiná právnická osoba, jedná-li při výkonu své působnosti, zapečetí dokument v elektronické podobě kvalifikovanou elektronickou pečetí.**

§9

- (1) K pečetění elektronickou pečetí lze použít **pouze uznávanou elektronickou pečeť**, pečetí-li se elektronický dokument, kterým se **právně jedná vůči veřejnoprávnímu podepisujícímu** nebo jiné osobě v souvislosti s výkonem jejich působnosti.
- (2) **Uznávanou elektronickou pečetí** se rozumí **zaručená elektronická pečeť založená na kvalifikovaném certifikátu pro elektronickou pečeť nebo kvalifikovaná elektronická pečeť**.

§ 10

- K pečetění elektronickou pečetí lze použít zaručenou elektronickou pečeť, uznávanou elektronickou pečeť, případně jiný typ elektronické pečeti, pečetí-li se elektronický dokument, kterým se právně jedná jiným způsobem než způsobem uvedeným v § 8 nebo § 9 odst. 1.

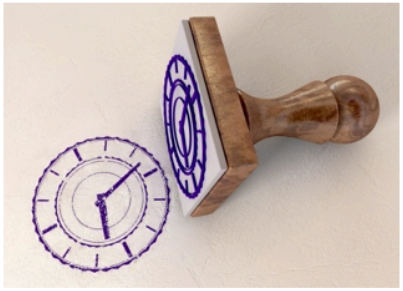
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Časové razítko dle 297/2016 Sb.

§11 Použití kvalifikovaného elektronického časového razítka

- (1) **Veřejnoprávní podepisující, který podepsal elektronický dokument**, kterým právně jedná, způsobem podle § 5, a osoba, která podepsala elektronický dokument, kterým právně jedná při výkonu své působnosti, způsobem **podle § 5, opatří podepsaný elektronický dokument kvalifikovaným elektronickým časovým razítkem**.

- (2) **Veřejnoprávní podepisující, který zapečetil elektronický dokument**, kterým právně jedná, způsobem podle § 8, a osoba, která zapečetila elektronický dokument, kterým právně jedná při výkonu své působnosti, způsobem podle § 8, opatří zapečetěný elektronický dokument kvalifikovaným elektronickým časovým razítkem.



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pozor na dodržování !

- Ačkoliv je zákon č. 297/2016 Sb. již rok platný a účinný od 19.9.2016 tak se stále nedodržuje u řady organizací !

- Řada organizací stále neplní zákonem stanovené povinnosti zejména:
  - §5 a §6 ohledně podepisování elektronických dokumentů
  - §8 a §9 ohledně elektronických pečetí (přechodně značek)
  - §11 ohledně časových razítek

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

eidentita.cz
KLÍČ K ELEKTRONICKÝM SLUŽBÁM

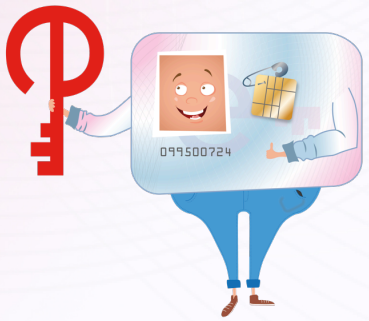
Zákon o elektronické identifikaci

- Zákon č. 250/2017 Sb. o elektronické identifikaci z 18.8.2017
- Zákon č.251/2017 Sb., kterým se mění některé zákony v souvislosti s přijetím zákona o elektronické identifikaci z 18.8.2017
- **§ 2 Prokázání totožnosti s využitím elektronické identifikace**
  - Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace **pouze prostřednictvím kvalifikovaného systému elektronické identifikace** (dále jen „kvalifikovaný systém“).

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Změna zákona o OP

- Novela zákona č.328/1999 Sb. o občanských průkazech
  - Vyhlášena ve sbírce 195/2017 dne 10.7.2017
  - změna souvisejících právních předpisů
  - zavádí jednotný eOP s čipem jako bezpečný prostředek podle nařízení eIDAS
  - zavádí se v novele 365/2000 Sb. tzv. přístup se zaručenou identitou a možnost subjektu údajů získat veškeré údaje z ISVS



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Změna zákona o ISVS

- Zákon č.104/2017 Sb., kterým se mění zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů, zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), a některé další zákony
  - sbírka zákonů částka 39 ze dne 5.4.2017 
  - účinnost od 1.7.2017
  - **informační koncepce pro orgány veřejné správy**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Změna zákona o ZR

- Zákon č.192/2016 , kterým se mění zákon č. 111/2009 Sb., o základních registrech, ve znění pozdějších předpisů, a některé další zákony
  - sbírka zákonů částka 72 ze dne 17.6.2016 
  - účinnost od 1.1.2017
  - další změny byly v souvislosti s „eOP“ a další se zákonem o „eID“
  - cílem je zajištění Národního bodu pro identifikaci, vydávání státních identifikačních a podpisových certifikátů pro „eOP“

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Zákon o archivnictví a SSL

- Zákon č.56/2014, kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů
  - sbírka zákonů částka 23 ze dne 7.4.2014

- Navazující vyhlášky
  - 259/2012 o podrobnostech výkonu spisové služby
  - 645/2004 provádějí některá ustanovení zákona o archivnictví a spisové službě a o změně některých zákonů
  - zveřejněn **4.7.2017 nový standard pro eSSL** 
    - **Věstník MV částka 57/2017**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Změna národního standardu eSSL

- Změna národního standardu pro eSSL přináší:
  - velké zjednodušení standardu, upřesňuje fáze „vzniku“ dokumentu - pojem rozpracovaný dokument (koncept)
  - podrobně popisuje **rozhraní mezi systémy eSSL a ostatními informačními systémy**
    - on-line propojení a off-line propojení
  - vzniká datový model „metadat“ dokumentu spisové služby
- Pozor – řada organizací nemá dlouhodobě IT systémy v souladu s národním standardem pro spisové služby !

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Stručný časový rámec

- 2016 služby vytvářející důvěru v praxi 
- 2017 právní předpisy a nástroje připravené MV
  - Novela zákona o eOP, zákon o eID
  - Do 31.12.2017 úprava vnitřních směrnic a pravidel pro ÚeP
- 2018
  - 25.5.2018 nařízení GDPR v účinnost
  - 1.7.2018 první nové eOP s čipem
  - 1.7.2018 účinnost zákona o eID
  - 29.9.2018 účinnost nařízení eIDAS , termín k ÚeP z usnesení Vlády ČR
    - oznámené systémy eID
    - usnesení realizovat možnost ÚeP
  - 31.12.2018 povinný příjem eFA v Evropském formátu a ISDOC 5.2 a vyšší

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

eID EU		**29.9.2018** akceptace eID oznámených	
eID CZ		1.7.2018 zahájení NIA	**1.7.2020** kde totožnost el. pouze NIA
ÚeP	31.12.2017 interní směrnice	**28.9.2018** realizovat možnost	
eFA	31.12.2017 interní směrnice	**31.12.2018** umožnění příjmu ISDOC	2019/2020 příjem EU eFA
GDPR	17 let platný 101/2000 Sb.	**25.5.2018** účinnost GDPR	

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

S rozvojem elektronických služeb se mění životní cyklus dokumentů

BUDE VÍCE E-DOKUMENTŮ

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Problematika k řešení

- Nárůst
  - množství elektronických dokumentů (co je el.dokument v eIDAS)
  - množství zpracování osobních údajů
- Rizika a hrozby
  - zneužití elektronických dokumentů nebo osobních údajů
  - zneužití elektronické „identity“
- Osvěta a vzdělanost
  - musíme více informovat, více metodicky pomáhat
  - dopady do oblasti vzdělávání

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Problematika k řešení

- „inteligentní elektronické dokumenty“
  - s ohledem na množství musíme **předem analyzovat dopady** na důvěryhodnost, autenticitu, velikost, možnost následného zpracování, bezpečnost a ochranu osobních údajů
  - e-dokumenty na „front-endu“ a „back-endu“
    - je třeba maximálně zefektivnit a zabezpečit „back-end“ pro výměnu, sdílení, zpracování a uchovávání elektronických dokumentů zejména pro e-governement, neboť řada údajů je zákonem vynucených a nikoliv dobrovolně poskytnutých
- maximální využití „privacy by design“, přístupu založeného na riziku, pseudoanonymizace a agregace před zveřejněním, šifrování apod.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pochopení terminologie je základ k porozumění problému a návrhu správných řešení

NĚKTERÉ DŮLEŽITÉ POJMY

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Nařízení eIDAS

I. podmínky pro uznávání eID v rámci oznámených systémů

II. pravidla pro služby vytvářející důvěru zejména u el.transakcí

III. právní rámec pro el. podpisy, el.pečetě, el.časová razítka, **elektronické dokumenty**, služby el.doporučeného doručování a certifikační služby pro autentizaci internetových stránek

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

eIDAS & e-dokument

- K elektronickému dokumentu
  - **„elektronickým dokumentem“** jakýkoli obsah uchovávaný v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka;
  - elektronickému dokumentu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu
  - Obecný pojmem dokument v zákoně č. 499/2004 Sb.
    - §2 písmeno e) **„dokumentem“** každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena;
    - §2 písmeno o) „**metadaty“** data popisující souvislosti, obsah a strukturu dokumentů a jejich správu v průběhu času

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Elektronické dokumenty

- Dokumenty jako nosič informace a osobních údajů
  - pozor na vlastnosti podle národní legislativy : 499/2004 Sb. §3 odst. 5) „V případě dokumentů v digitální podobě se jejich uchováváním rozumí **rovněž zajištění věrohodnosti původu dokumentů, neporušitelnosti jejich obsahu a čitelnosti, tvorba a správa metadat náležejících k těmto dokumentům v souladu s tímto zákonem a připojení údajů prokazujících existenci dokumentu v čase**. Tyto vlastnosti musí být zachovány **do doby provedení výběru archiválií**.
  - elektronické dokumenty mohou být nosičem osobních údajů
  - do doby skartačního řízení nelze realizovat právo na výmaz

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

eIDAS x GDPR

- Preambule (11)
  - Toto nařízení by mělo být uplatňováno v plném souladu **se zásadami ochrany osobních údajů podle směrnice Evropského parlamentu a Rady 95/46/ES**. V tomto směru by se, s ohledem na zásadu vzájemného uznávání stanovenou v tomto nařízení, měla autentizace pro účely on-line služeb týkat zpracování pouze těch identifikačních údajů, které jsou přiměřené, podstatné a rozsahem úměrné pro udělení přístupu k dané on-line službě. Dále by poskytovatelé služeb vytvářejících důvěru a orgány dohledu měly dodržovat požadavky stanovené ve směrnici 95/46/ES týkající se důvěrné povahy a bezpečnosti zpracování.
  - viz dále i čl. 5 odst. 1

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

eIDAS x GDPR

- Preambule (31)
  - orgány dohledu by měly spolupracovat s orgány pro ochranu údajů, například je informovat o výsledcích auditů kvalifikovaných poskytovatelů služeb vytvářejících důvěru, jestliže podle všeho došlo k porušení pravidel týkajících se ochrany osobních údajů. Toto poskytování informací by se mělo týkat zejména bezpečnostních incidentů a narušení bezpečnosti osobních údajů.
  - k tomu dále pak viz čl. 14 odst.4 písm. f)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

eIDAS x GDPR

- Čl. 19
  - 2. Kvalifikovaní a nekvalifikovaní poskytovatelé služeb vytvářejících důvěru **vyrozumí orgán dohledu a případné další příslušné subjekty, jako jsou příslušný vnitrostátní orgán pro bezpečnost informací nebo orgán pro ochranu údajů**, o každém narušení bezpečnosti nebo ztrátě integrity, jež mají významný dopad na poskytovanou službu vytvářející důvěru nebo na uchovávané osobní údaje, a to bez zbytečného odkladu a v každém případě do 24 hodin od okamžiku, kdy toto narušení zjistili
  - k tomu též čl. 20 odst. 2

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Srpen - Listopad 2017

AKTUÁLNÍ UDÁLOSTI

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Aktuální stav

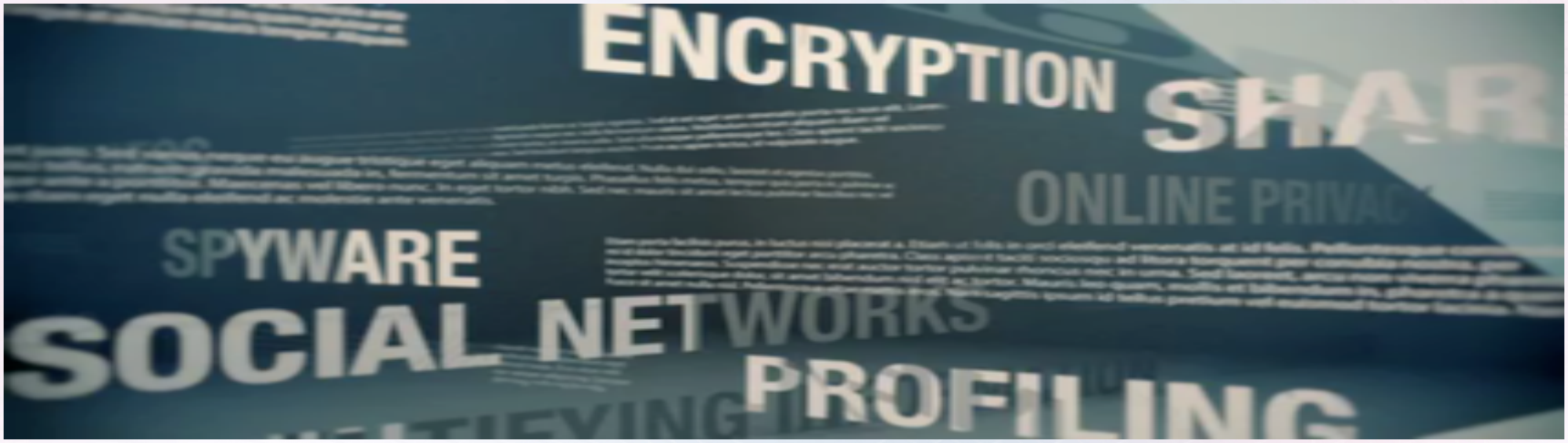
- Srpen/Září 2017
  - Ministerstvo vnitra vydalo:
    - Metodické doporučení k pověřenci pro obce
    - Pověřenci ochrany osobních údajů ve služebních úřadech – metodické doporučení
    - Nový návrh zákona nahrazující zákon č. 101/2000 Sb. zpracování připomínek z vnějšího připomínkového řízení = v termínu k 25.5.2018 patrně nebude nový zákon

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Aktivity současné

- Listopad 2017
  - Koordinátor pro digitální agendu
    - Konference 6.11.2017 v Lichtenštejnském paláci
      - Metodika k pověřencům
      - Nástroje eGovernmentu x GDPR
      - Kybernetická bezpečnost x GDPR
    - Semináře 7.11.2017 v Hrzánském paláci
      - e-fakturace, ÚeP, spisová služba
      - architektonické principy

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



GDPR není REVOLUCE ale EVOLUCE!

DOPADY GDPR

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Výchozí stav

- Zákon č.101/2000 Sb. o ochraně osobních údajů
  - Správce povinen §5
    - stanovit účel, k němuž mají být osobní údaje zpracovány
    - stanovit prostředky a způsob zpracování osobních údajů
    - shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanoveného účelu
    - uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu zpracování
    - zpracovávat pouze v souladu se zákonem, udržovat je přesné
    - zpracovávat osobní údaje pouze v souladu s účelem ….
- Kdo zcela splňuje požadavky zákona bude mít snadnou adaptaci, řada organizací ale nesplňuje požadavky!

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pojem osobní údaj

- Zákon č.101/2000 Sb.
  - osobním údajem **jakákoliv informace týkající se určeného nebo určitelného subjektu údajů**. Subjekt údajů se považuje za určený nebo určitelný, jestliže lze subjekt údajů přímo či nepřímo identifikovat zejména na základě čísla, kódu nebo jednoho či více prvků, specifických pro jeho fyzickou, fyziologickou, psychickou, ekonomickou, kulturní nebo sociální identitu
- Nařízení GDPR – článek 4 odst. 1)
  - „osobními údaji“ **veškeré informace o identifikované nebo identifikovatelné fyzické osobě** (dále jen „subjekt údajů“); identifikovatelnou fyzickou osobou je fyzická osoba, **kterou lze přímo či nepřímo identifikovat**, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity této fyzické osoby;

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Definice pojmů nařízení GDPR

- **Zpracování**
  - jakýkoli úkon nebo soubor úkonů s osobními údaji, které jsou prováděny pomocí či bez pomoci automatizovaných postupů, jako je shromažďování, zaznamenávání, uspořádávání, strukturování, uchovávání, přizpůsobování nebo pozměňování, vyhledávání, konzultace, použití, sdělení prostřednictvím přenosu, šíření nebo jakékoli jiné zpřístupnění, srovnání či kombinování, jakož i blokování, výmaz nebo likvidace
- **Pseudonymizací**
  - zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě;

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Nové přístupy - GDPR

- Nařízení GDPR
  - **přístup založený na riziku**
    - že správce již od počátku koncipování zpracování osobních údajů musí brát v potaz povahu, rozsah, kontext a účel zpracování a přihlédnout k pravděpodobným rizikům pro práva a svobody fyzických osob a tomu musí přizpůsobit i zabezpečení osobních údajů
    - Nové povinnosti – ohlašování (oznamování) případů porušení zabezpečení OÚ, posuzování vlivu na zpracování OÚ, konzultace s ÚOOÚ
  - **princip odpovědnosti správce**
    - odpovědnost správce za dodržení zásad zpracování, které jsou uvedeny v článku 5 odst. 1 a doložení souladu (kodexy, certifikace, záznamy o činnostech zpracování..)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

GDPR a veřejná správa

- Nové povinnosti
  - záznamy, prokazování souladu, pověřenec, řešení incidentů, DPIA
- Žádosti subjektů
  - nárůst žádostí o výkon práv
- Pozor nezapomenout na zaměstnance
  - zpracování údajů zaměstnanců
- Dopady na smlouvy (i existující)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Záměrná a standardní ochrana

- S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k pravděpodobným rizikům pro práva a svobody fyzických osob, jež s sebou zpracování nese, zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování samotného vhodná technická a organizační opatření, jejichž účelem je:
  - provádět zásady ochrany údajů účinným způsobem a
  - začlenit do zpracování nezbytné záruky, tak aby splnil požadavky tohoto nařízení a ochránil práva subjektů údajů.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Záměrná a standardní ochrana

- vhodná technická a organizační opatření:
  - minimalizace zpracování osobních údajů,
  - co nejrychlejší pseudonymizace osobních údajů,
  - transparentnost s ohledem na funkce a zpracování osobních údajů,
  - umožnění subjektům údajů monitorovat zpracování osobních údajů a
  - umožnění správcům vytvářet a zlepšovat bezpečnostní prvky (zhotovitelé produktů, služeb a aplikací)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Záměrná a standardní ochrana

- povinnost posuzovat vliv jednotlivých zpracování a vyžádat si předběžnou konzultaci u dozorového úřadu
- povinnost posouzení pro systematické a rozsáhlé vyhodnocování osobních aspektů, na němž se zakládají rozhodnutí s právními účinky, pro rozsáhlé systematické monitorování veřejně přístupných prostorů a rozsáhlé zpracování citlivých údajů

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Přístup založený na riziku

- Základ pro nastavování povinností správce je rizikovost
  - dovozována z rozsahu zpracování, zpracovávaných osobních údajů (citlivé údaje)a používaných technologií

- S přihlédnutím ke stavu techniky, nákladům, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody, jež sebou zpracování nese
  - zavede správce jak v době určení prostředků pro zpracování, tak v době zpracování vhodná technická a organizační opatření a začlení do zpracování nezbytné záruky.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Posouzení vlivu

- Posouzení je nutné zejména v těchto případech:
  - systematické a rozsáhlé vyhodnocování osobních aspektů fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí s právními účinky nebo mají na fyzické osoby podobně závažný dopad
  - rozsáhlé zpracování zvláštních kategorií údajů (citlivé)nebo údajů týkajících se rozsudků v trestních věcech a trestných činů
  - rozsáhlé systematické monitorování veřejně přístupných prostorů

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Předávání údajů - cizina

- Hodnocení třetí země (Komise)
  - zásady právního státu, standardy lidských práv, nezávislý dozor, mezinárodní závazky.
- Předávání založená na vhodných zárukách
- Výjimky
  - subjekt údajů byl informován o možných rizicích, která pro něj v důsledku absence rozhodnutí o odpovídající ochraně a vhodných záruk vyplývají, a k navrhovanému předání vydal svůj výslovný souhlas
- Předání, která nejsou opakovaná, omezený počet subjektů údajů
  - lze uskutečnit pro účely závažných oprávněných zájmů správce, pokud nad těmito zájmy nepřevažují zájmy/práva a svobody subjektu údajů

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pseudonymizace

- Osobní údaje již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, uchovávaných odděleně a technická a organizační opatření zajišťují, že nebudou přiřazeny identifikované/identifikovatelné fyzické osobě
- Vhodná záruka:
  - snižuje rizika pro práva subjektu údajů
  - změkčuje některé povinnosti správců (a zpracovatelů): práva subjektu údajů podmíněna schopností správce subjekt údajů identifikovat

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Nové funkce v IT systémech

- Nařízení GDPR upravuje podrobněji:
  - **právo na opravu** dle článku 16, kdy subjekt údajů má právo na to, aby správce bez zbytečného odkladu opravil nepřesné osobní údaje
  - **právo na výma**z dle článku 17, kdy subjekt údajů má právo na to, aby správce bez zbytečného odkladu vymazal osobní údaje, které se daného subjektu údajů týkají
  - **právo na přenositelnost** dle článku 20, kdy subjekty údajů jsou oprávněny získat osobní údaje, které poskytly správci ve strukturovaném, běžně používaném a strojově čitelném formátu a předat je jinému správci
  - Povinnost správce napomáhat uplatňování práv (on-line, hot-line…)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady na IT

- Architektura IT řešení by měla kromě architektonických postupů a shodou s NAP obsahovat s ohledem na GDPR zejména pak:
  - principy „**Privacy by design**“ tj. ochranu soukromí již od návrhu
    - zaměřené na subjekt, objekt, transakci, systém
    - proaktivní (prevence nikoliv náprava), minimalismus dat, ochrana již v návrhu, plná funkčnost, bezpečnost od začátku do konce, stálá otevřenost (transparentnost a viditelnost), soukromí uživatele
  - kontinuální proces – nejedná se o jednorázový soulad, ale o trvalý děj

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Fáze implementace GDPR

Analýza

Analýza současného stavu x rozdíly od 25.5.2018

Implementace

Úpravy směrnic, smluv, systémů a organizačních opatření

Udržitelnost systému

Zajištění organizačně-technických opatření v čase

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Další dopady GDPR na IT

- Nutno zajistit vedení některých nových „agend“
  - v rámci eSSL evidovat „požadavky“ od subjektu údajů
  - při obnově dat ze záloh kontrolovat oproti evidenci uplatněných práv na výmaz
  - některé činnosti lze částečně nebo zcela automatizovat
    - s využitím elektronické identifikace lze připravit on-line služby pro řešení některých situací
    - typicky právo na přenositelnost lze zcela automatizovat
  - pozor na záznamy o zpracování

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady nejen na IT

- Revidování smluv se zpracovateli / externími dodavateli
  - je zcela nutné inventarizovat veškeré smlouvy (jak na informační systémy, tak i na jiné externí služby související s činnostmi, kde se pracuje s osobními údaji)
  - provést analýzu smluv a navrhnout změny v souvislosti s GDPR
  - možná pomoc ÚOOÚ x pověřenec
- Revidování smluv se zaměstnanci
  - pozor na některé agendy v personalistice

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady na smlouvy

- Problematika revize smluv x GDPR
  - smlouvy musí jasně nastavit povinnosti a odpovědnost za případnou škodu jednotlivých smluvních stran s ohledem na zpracování osobních údajů
  - pro externí zpracování doporučení smluvně upravit, že externí zpracovatel zpracovává OÚ v souladu s nařízením a obecně platnými právními předpisy
  - pozor na “zřetězení“ smluv (systémový integrátor x skutečný realizátor x fyzické umístění atd..)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Nové požadavky na smlouvy

- Dopad na dodavatele IT systémů s přístupem k údajům
- Due diligence před uzavřením
  - Dostatečné záruky zavedení vhodných technických a organizačních opatření
- Zpracování pouze dle pokynů správce
  - Výjimky dle práva EU a členských států
  - Informování o požadavcích zákona
- Bezpečnostní opatření
- Součinnost při zabezpečení, hlášení incidentů, atd.
- Infomační povinnost
- Audity, včetně prohlídek na místě

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady v souvislostech

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady GDPR x zákon č.250/2017

- Zákon č. 250/2017 o elektronické identifikaci
  - není nutné provádět hodnocení dopadů, návrh zákona obsahoval hodnocení dopadů na ochranu osobních údajů
  - správce NIA je SZR, kvalifikovaných systémů jsou kvalifikovaní správci
  - rozsáhlé zpracování osobních údajů, zpracovávají a uchovávájí se OÚ
    - např. §21, §22 …
  - právo na přenositelnost osobních údajů
    - §21 odst. 3) „v národním bodu se dále mohou vést údaje, které poskytne držitel.“

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Druhy dokumentů a dopady

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

GDPR a eSSL

- §64 příjem, označování, evidence a rozdělování dokumentů
  - odst.4) „jmenný rejstřík“ určený pro vyhledávání, ověřování a automatické zpracování údajů o adresách odesílatelů a adresátech dokumentů evidovaných v evidenci
  - jmenný rejstřík může pomoci v některých případech
- eSSL s podporou fulltextového vyhledávání
- eSSL je hlavní evidenční systém & „řídí“ skartační řízení
  - správně stanovené skartační lhůty jsou základem pro např. uplatnění práva na výmaz

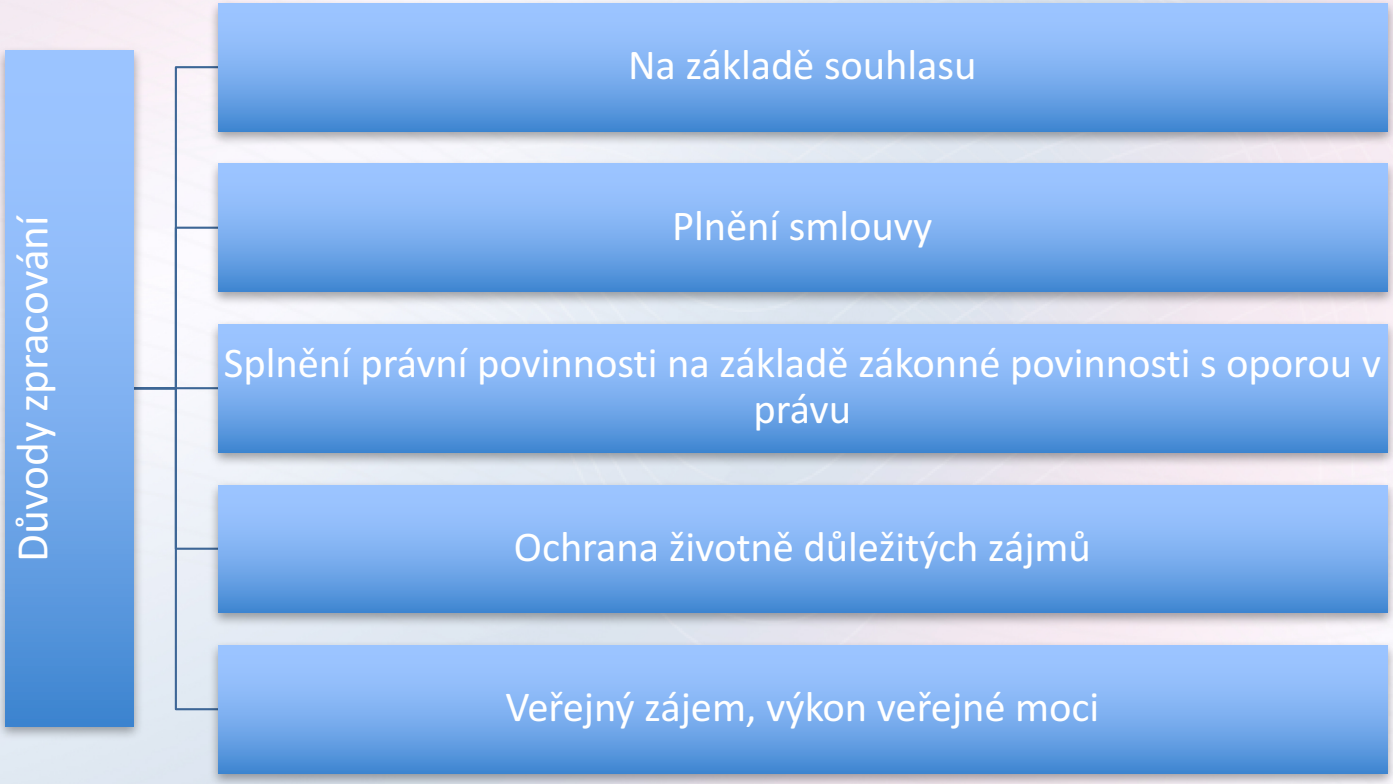
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

GDPR a fakturace

- Dopady GDPR na faktury
  - faktury mohou obsahovat a obvykle obsahují řadu osobních údajů
    - např. vystavil, dále pak adresní část, kdo převzal fakturu a podobně
  - většinou bude zpracování spojeno s plněním nějaké povinnosti
    - např. zákon o účetnictví, daňové zákony a podobně
    - nutno správně nastavit skartační lhůty a dále pak proces skartačního řízení
      - pokud bude nevhodně nastaveno je nutné počítat s možností uplatnění práva na výmaz
  - v souvislosti se zpracováním mohou být v rámci životního cyklu faktury připojeny osobní údaje zaměstnanců zpracovatele
  - u elektronických faktur dochází většinou k automatizovanému zpracování

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Právní důvody zpracování



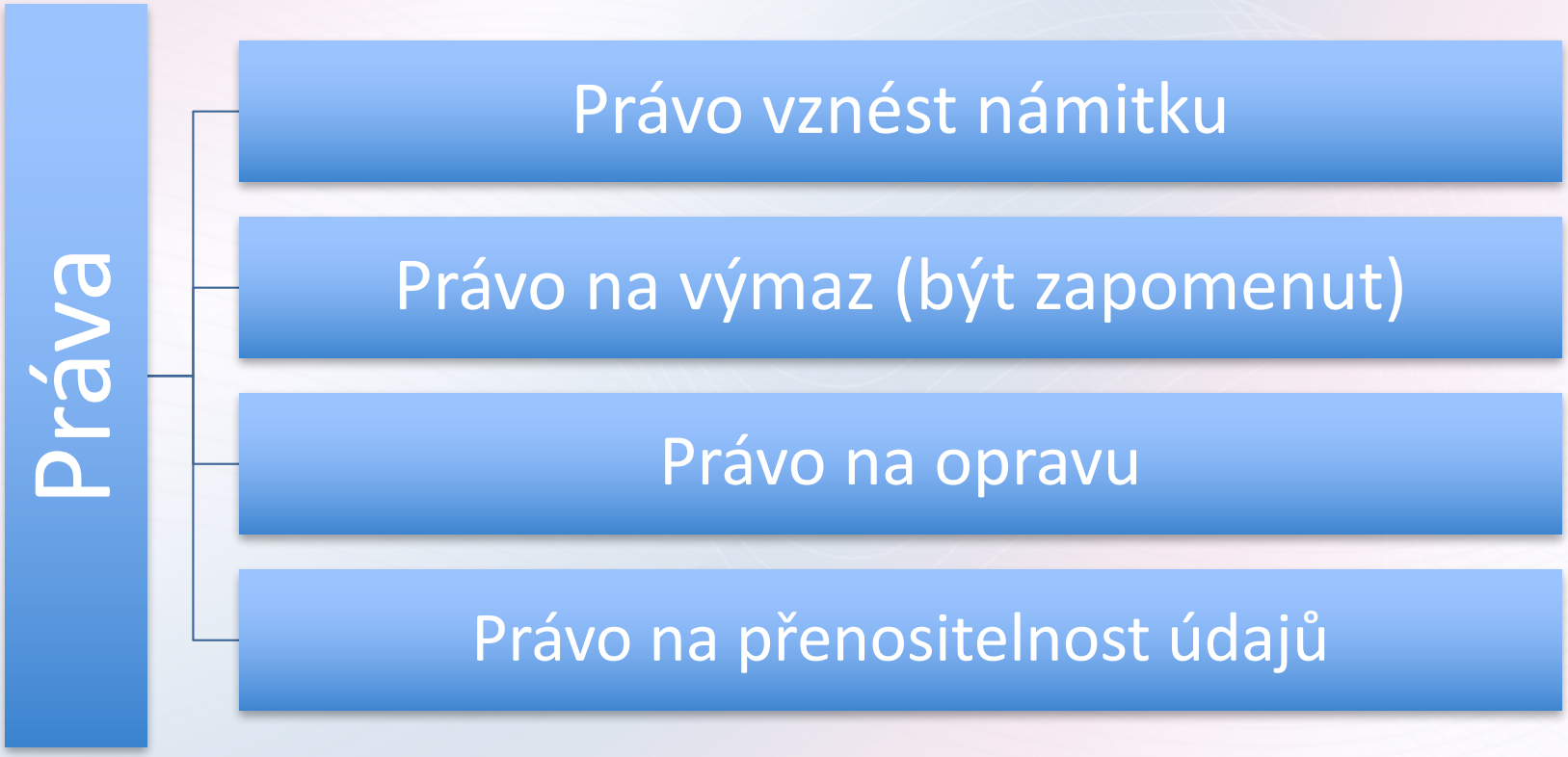
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady na IT a procesy

- Revidovat souhlasy se zpracováním OU
  - např. nelze „před-vyplňovat“ nebo podmiňovat přístup k online službám
- Analyzovat chování IT systémů podle titulu
  - na základě „souhlasu“
  - na základě „smlouvy“
    - pozor na exit strategii, pokud generální souhlas pak alespoň notifikace a námitka
  - na základě „právní povinnosti správce“
    - musí vyplývat z práva ČR nebo EU, pozor na správně nastavené skartační lhůty
  - ve veřejném zájmu

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Nová práva fyzických osob



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

GDPR má vždy dopady na IT

- Dopady GDPR na IT systémy
  - právo na přenositelnost údajů dle čl.20
    - v některých případech bude nutné upravit IT systémy aby se nemuselo „dělat“ ručně
  - právo na výmaz dle čl.17
    - dopady na strategii zálohování a obnovy dat – kde bylo uplatněno právo na výmaz nelze při obnově „obnovit“ tato data do produktivního prostředí
    - nepřímé dopady na analýzu všech skartačních lhůt u zpracování u veřejnoprávních původců
  - právo na přístup k osobním údajům dle čl.15
    - pozor např. u Smart-Cities – zapomíná se často na dopady ochrany osobních údajů
    - pozor u předávání do třetích zemí nebo mezinárodním organizacím – právo na informace o vhodných zárukách

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Právo na výmaz & zálohy

1. • Agenda – evidence práv na výmaz
2. • Obnova dat do neproduktivního prostředí, opětovné „smazání dat dle evidence práv na výmaz“
3. • Obnova dat podle bodu 2. do produktivního prostředí

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

„Nevděk je znamení slabosti. Nikdy jsem neviděl schopné lidi, kteří by byli nevděčni.“

Johann Wolfgang von Goethe

POVĚŘENEC

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Kdo je pověřenec?

- **Data Protection Officer -** Pověřenec na ochranu osobních údajů
  - smyslem tohoto institutu je zvýšit odpovědnost správce, zajistit lepší plnění předpisů pro ochranu osobních údajů a roli prostředníka mezi správcem, subjektem údajů a dozorovým orgánem
  - pověřenec má rozvíjet kulturu ochrany osobních údajů uvnitř organizace a pomáhat zavádět její klíčové prvky
  - pověřenec nepřebírá odpovědnost za správce. Správce sám musí podle čl. 24(1) Obecného nařízení zajistit i doložit, že (jeho zaměstnanci) plní povinnosti podle Obecného nařízení

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pověřenec

- **Pověřenec pro ochranu osobních údajů – článek 37**
  - jmenování pověřence
    - ✓ správce a zpracovatel
  - postavení pověřence
    - ✓ správce a zpracovatel zajistí, aby pověřenec nedostával žádné pokyny týkající se výkonu úkolů
  - úkoly pověřence
- **Pro orgány veřejné moci povinnost !**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

WP29 – vodítka POOÚ

- Vodítka k pověřencům pro ochranu osobních údajů
  - jmenování pověřence
  - postavení pověřence
  - úkoly pověřence
  - příloha – co potřebujete vědět?
    - kdo musí mít pověřence
    - zdroje pro pověřence
    - konflikt zájmů

… a další doporučení

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Úkoly pověřence

- Hlavní úkoly pověřence:
  - Poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, kteří provádějí zpracování, o **jejich povinnostech podle tohoto nařízení** a dalších předpisů Unie nebo členských států v oblasti ochrany údajů;
  - **Monitorování souladu s tímto nařízením, dalšími předpisy Unie nebo členských států v oblasti ochrany údajů a s koncepcemi správce nebo zpracovatele** v oblasti ochrany osobních údajů, **včetně rozdělení odpovědnosti**, zvyšování povědomí a odborné přípravy pracovníků zapojených do operací zpracování a souvisejících auditů;

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Úkoly pověřence

- Další úkoly pověřence:
  - Poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35;
  - **Spolupráce s dozorovým úřadem**
  - Působení jako **kontaktní místo pro dozorový úřad** v záležitostech týkajících se zpracování, včetně předchozí konzultace podle článku 36, a případně vedení konzultací v jakékoli jiné věci.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pověřenec

- Schopnost plnit úkoly:
  - postavení v organizaci
  - klíčová osoba při rozvoji kultury ochrany dat, pomáhá zavádět nařízení
  - musí mít dostatečnou samostatnost a zdroje pro efektivní výkon funkce
  - dostupnost (hot-line, osobní dostupnost)
  - POZOR na střet zájmů – nelze formálně obejít např. na vedoucího pracovníka IT a podobně!

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Střet zájmů & pověřenec

Střet zájmů:

- určit pracovní místa neslučitelná s výkonem funkce pověřence
- sestavit vnitřní pravidla k zamezení střetu zájmů
- začlenit do pravidel obecnější vysvětlení střetu zájmů
- analyzovat případný střet pověřence dle smlouvy – interní x externí

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Pověřenec – konflikt zájmů WP29

- Existuje několik záruk umožňujících pověřenci konat nezávisle:
  - **žádné pokyny** od správce nebo zpracovatele **týkající se výkonu úkolů** pověřence
  - **nemožnost propuštění nebo sankcionování** v souvislosti s plněním úkolů
  - zajištěním správcem nebo zpracovatelem, aby **žádné pověřencovy úkoly nebo povinnosti nevedly ke střetu zájmů**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Co nesmí pověřenec – WP29

- Pověřenec dle doporučení WP 29
  - pověřenec nemůže v organizaci zastávat místo, na kterém by musel **stanovovat účely a prostředky zpracování osobních údajů**
  - v konfliktním postavení uvnitř organizace mohou typicky být pozice ve vyšším managementu (výkonný ředitel, provozní ředitel, finanční ředitel, zdravotní ředitel, vedoucí marketingového oddělení, vedoucí personálního oddělení nebo vedoucí oddělení IT), ale i pozice na nižším stupni organizační struktury, **pokud v takovém postavení dochází k rozhodování o účelech a prostředcích zpracování**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Více souvisejících organizací

S ohledem na charakter nařízení a výše uvedených doporučených činností:

1. „zastřešující organizace“ by měla resortním organizacím poskytnout minimálně metodickou a konzultační podporu v souvislosti s implementací nařízení GDPR;
2. optimální stanovení počtu pověřenců na ochranu osobních údajů (lze mít pro více organizací „sdíleného“ pověřence, pokud to bude možné s ohledem na charakter jeho funkce;
3. v rámci celku lze u stejných typů organizací zavést stejné postupy (typicky například problematika GDPR u měst a obcí).

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Shrnutí k pověřenci

- Pověřenci nenesou osobní odpovědnost za nedodržování GDPR – vždy správce nebo zpracovatel
- Správce nebo zpracovatel mají klíčovou úlohu pro vytváření podmínek pověřenci
- Musí být snadno dosažitelný a musí být schopen komunikovat v jazyce užívaných orgánů dozoru a subjektem údajů
- Podle článku 37 odst.5 musí mít profesní kvality a musí být schopen plnit úkoly dle nařízení
- „Pokyny k funkci pověřence …“ WP 29 – z 13.12.2016 a “Často kladené otázky“

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Shrnutí k pověřenci

- Metodika MVČR pro obce obsahuje i obecná doporučení
  - pověřenec zaměstnanec – úředník dle zákona č.312/2002 Sb., obsazení dle §4 a následujících
  - pověřenec externí - §1746 odst.2 zákona č. 89/2012 Sb.
  - pozor na zastupování v době nepřítomnosti – musí splňovat všechny předpoklady i zástupce

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Slovo závěrem

„Kdo systematicky dodržuje právní předpisy zejména v oblasti ochrany osobních údajů, evidence dokumentů a vedení spisové služby, zákona o službách vytvářejících důvěru pro elektronické transakce a má správně nastavené smlouvy s IT dodavateli nebude mít problém i s ohledem na výrazný nárůst elektronických dokumentů a související nárůst nových povinností.“

„U ostatních může být GDPR příslovečná poslední kapka – proto nenechejte nádobu přetéci - stále ještě je čas na nápravu!“

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Ing.Robert Piffl, e-mail: robert.piffl@mvcr.cz

DĚKUJI VÁM ZA POZORNOST !