MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

E-dokumenty v souvislosti s nařízeními eIDAS a GDPR

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 MO MV*
- *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 1.4.2018*

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

„DOPADY EVROPSKÉ A ČESKÉ LEGISLATIVY NA ICT, aneb jak správně pracovat s elektronickými dokumenty, elektronickou identitou a dalšími nástroji e-governmentu“

ÚVOD

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Legislativní východiska

- 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

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

Evropské nařízení eIDAS a GDPR

NAŘÍZENÍ EU

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

Pojmy v rámci nařízení EU

- Řada pojmů je zcela jasně definována v nařízení eIDAS a GDPR
  - zvýšení přehlednosti práva a standardizace v rámci EU
  - **nelze je jinak vykládat nebo upravovat na národní úrovni**
  - definuje přesně klíčové pojmy v oblasti elektronické identifikace, elektronických dokumentů, podepisování, pečetění, razítkování časovými razítky atd. …
  - výše uvedené společně s národní úpravou zákona č. 297/2016 má zcela zásadní dopady i na oblasti, které případně národní legislativa „nestihla uvést v soulad s nařízeními“ – nařízení mají přednost

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

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

Právní účinky e-dokumentu

- článek 46 Právní účinky elektronických dokumentů
  - 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

- Výše uvedený právní účinek napříč EU je zcela zásadním východiskem pro „elektronické podání, elektronické úřadování a celý životní cyklus elektronického dokumentu"

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Účinnost nařízení eIDAS pro eID

- Klíčové datum 29.9.2018 – účinnost nařízení eIDAS pro elektronickou identifikaci
- „**Pokud se** podle vnitrostátního práva nebo správní praxe pro přístup ke službě poskytované on-line subjektem veřejného sektoru **v určitém členském státě vyžaduje elektronická identifikace s použitím prostředku pro elektronickou identifikaci a autentizace**, je **pro účely přeshraniční autentizace pro danou on-line službu uznán v tomto členském státě** prostředek pro elektronickou identifikaci **vydaný v jiném členském státě**, pokud jsou splněny tyto podmínky … „

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

GDPR není REVOLUCE ale EVOLUCE!

NAŘÍZENÍ GDPR

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, nový zákon bude později !**

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;

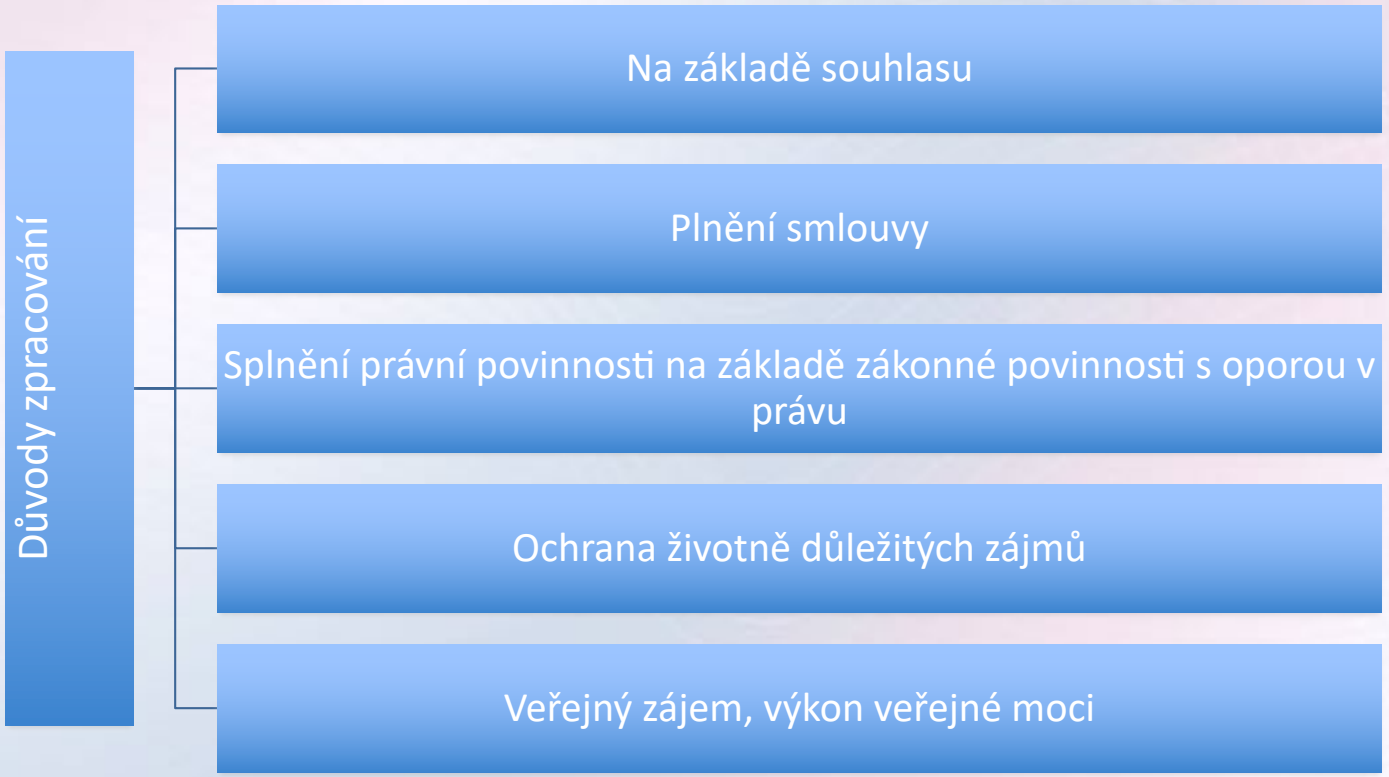
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

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

Právní důvody zpracování



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

Nové a změněné právní předpisy, příprava budoucích úprav

NÁRODNÍ LEGISLATIVA CZ

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**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Služby vytvářející důvěru

Elektronické podpisy

- Pouze fyzické osoby
- Kvalifikované podpisy je vždy vyžadován znalostní kód
- Pro ověření je potřeba provést test v některých případech 2 x po 24 hodinách

Elektronické pečetě

- Pouze právnické osoby
- Kvalifikované vyžadují certifikované prostředky
  - Zatím pouze jeden HW v EU
- Lze přiřadit automatizovaně na pozadí

Časová razítka

- Pozor na lhůty platnosti
- Lze provádět sumarizace a razítkovat pouze souhrnné protokoly

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

Definice pojmů 297/2016 Sb.

- Uznávaný podpis
  - §6 odst.2) „Uznávaným elektronickým podpisem se rozumí **zaručený elektronický podpis založený na kvalifikovaném certifikátu** pro elektronický podpis nebo **kvalifikovaný elektronický podpis**.“
  - POZOR – 19.9.2018 končí přechodná lhůta pro současné podpisy a značky

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

Konec přechodného období

- **Dne 19.9.2018 končí přechodná doba pro možnost používání zaručených elektronických podpisů, pečetí a časových razítek**
- § 19 Přechodná ustanovení
  - (1) **Po dobu 2 let** ode dne nabytí účinnosti tohoto zákona lze k podepisování podle §5 **použít rovněž zaručený elektronický podpis** založený na kvalifikovaném certifikátu pro elektronický podpis.
  - (2) **Po dobu 2 let** ode dne nabytí účinnosti tohoto zákona lze namísto zaručené elektronické pečetě založené na kvalifikovaném certifikátu pro elektronickou pečeť nebo **namísto kvalifikované elektronické pečetě** použít … písmeno a) + b)
  - (3) Pro účely odstavce 2 se §11 odst. 2 použije obdobně.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ELEKTRONICKÁ IDENTIFIKACE FO

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

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

identita.cz
KLÍČ K ELEKTRONICKÝM SLUŽBÁM

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Definice pojmů 250/2017 Sb.

- **§ 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

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Občanský průkaz po 1.7.2018

Státem vydávaný průkaz totožnosti a klíč k e-Government službám

- průkaz totožnosti
- veřejná listina
- I.etapa obsahuje eID
- II.etapa obsahuje státní kvalifikovaný podpis

- pro využití eOP s čipem potřebuji:
  - osobní počítač
  - čtečku čipových karet
  - připojení k internetu
  - aktivovaný identifikační certifikát

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
    - off-line propojení
  - vzniká datový model „metadat“ dokumentu spisové služby

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Konec přechodného období

- Národní standard pro eSSL uveřejněný dne 4.7.2017 plně nabývá účinnosti od 4.7.2018

- Národní standard pro eSSL bude novelizován v roce 2018 v souvislosti se změnami vyplývajícími z nového zákona o ochraně osobních údajů - může být až po uveřejnění nového zákona ve sbírce

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Metodické materiály MVCR

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Sekce GDPR na webu MVCR

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

S rozvojem elektronických služeb se mění životní cyklus dokumentů

ELEKTRONICKÉ DOKUMENTY

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Role e-dokumentu

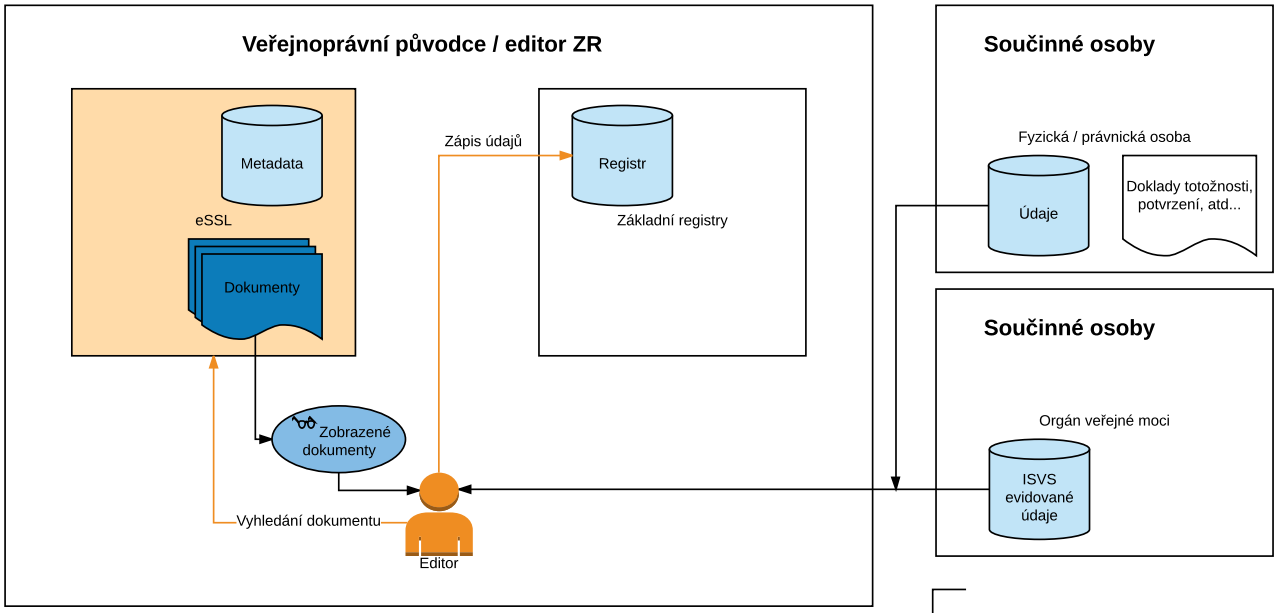
- „základní stavební kámen“ pro elektronizaci a digitalizaci
- nosič osobních údajů
- nosič písemně zaznamenané informace v elektronické podobě
- měl by nahradit „papír“ v e-světě …
- elektronická faktura, daňový doklad v elektronické podobě, účetní záznam v technické formě, písemná smlouva v e-podobě atd…

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dokument je základní předpoklad pro správnou funkcionalitu ZR

E-DOKUMENT & ZÁKON 365/2000

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



111/2009 Sb. § 4 odst. 2) **Editor** je zodpovědný za to, že jím **zapsané referenční údaje** jsou v **souladu s údaji uvedenými v dokumentech, na jejichž základě jsou údaje do příslušného základního registru zapsány**; orgány veřejné moci, fyzické a právnické osoby jsou povinny poskytnout editorovi potřebnou součinnost k plnění jeho úkolů tím, že mu poskytnou údaje a podklady potřebné pro ověření správnosti zpracovávaných údajů.

111/2009 Sb. § 3 - zápis nejpozději do pracovních 3 dnů ode dne, kdy se o vzniku nebo změně skutečnosti dozví

Zápis probíhá výhradně na základě dokumentů !

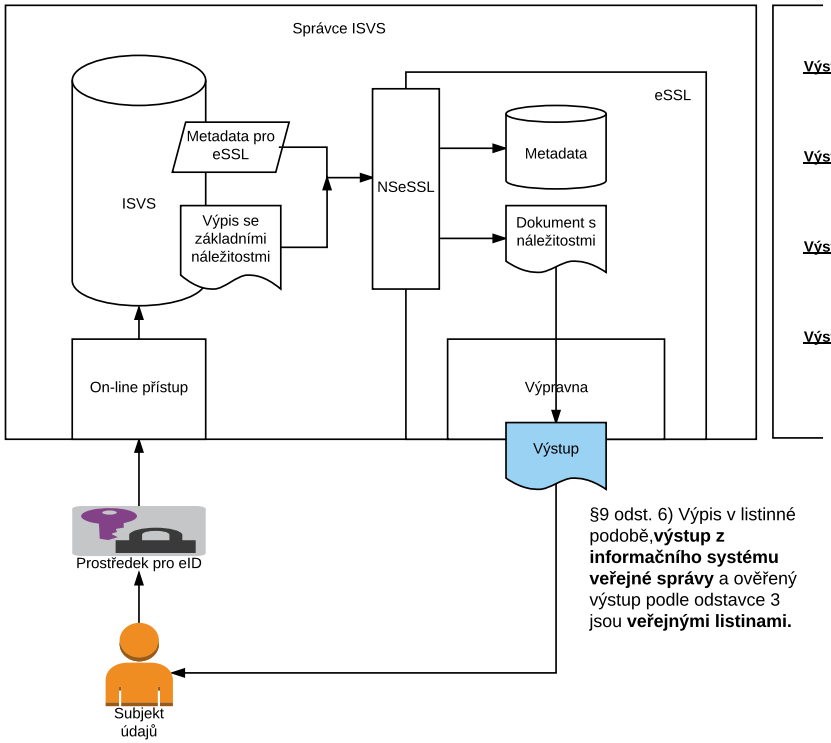
Záznamy o přístupech - 2 roky úschova

Otázky:

a) jak dlouho se uchovávají dokumenty na základě nichž, se údaje zapisují?

b) co údaje+podklady od součinných osob ?

- **kopie dokladů**
- **kopie podkladů**



Výstup z ISVS v rámci on-line služby je:

a) veřejná listina
b) elektronický dokument

Výstup z ISVS je:

a) dokument vyhotovený původcem dle §16 259/2012 Sb.
b) původce zajistí veškeré náležitosti podle zákona 499/2004 Sb.

Výstup z ISVS musí být opatřen:

a) náležitostmi dle příslušného procesní právní úpravy
- např. dle správního řádu, dle OSŘ a podobně.

Výstup z ISVS = právní jednání

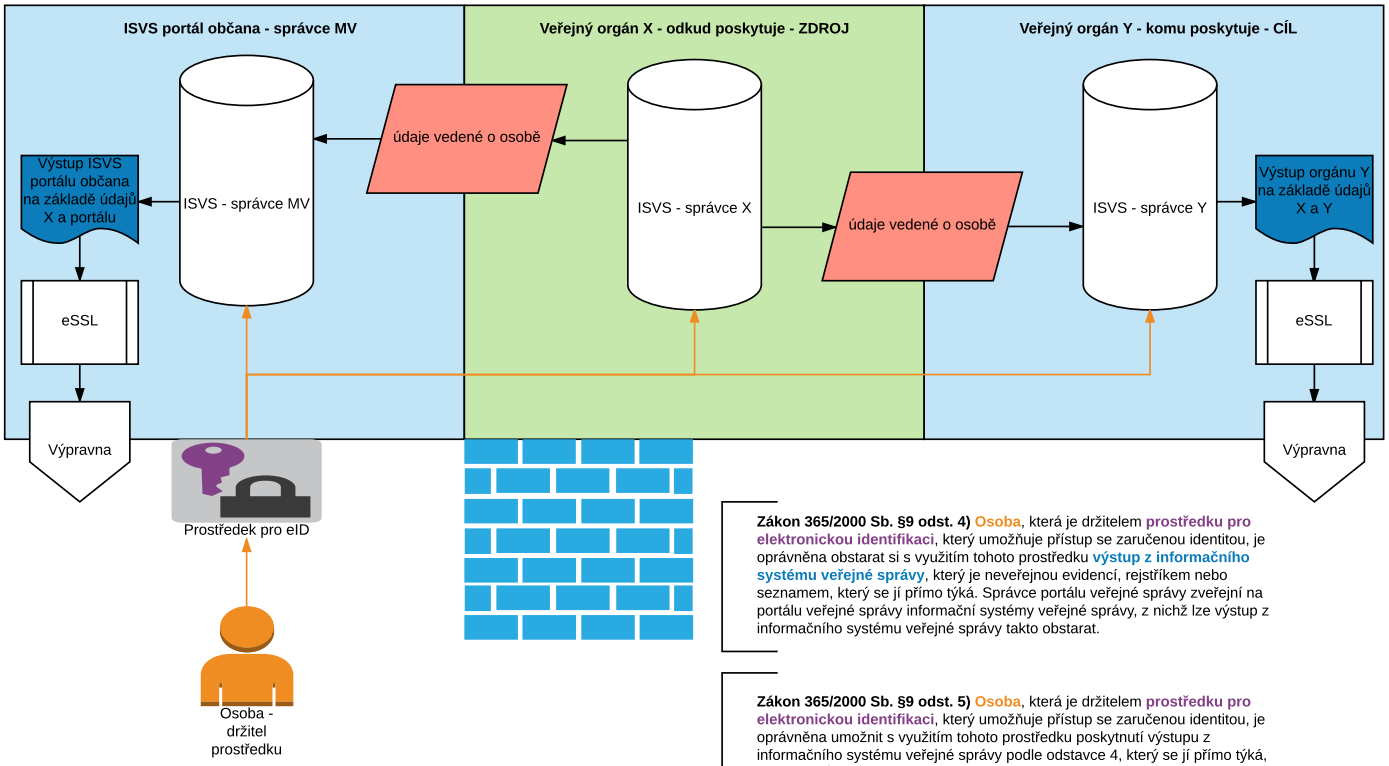
a) nutno opatřit náležitostmi dle 297/2016 Sb.

§9 odst. 6) Výpis v listinné podobě,**výstup z informačního systému veřejné správy** a ověřený výstup podle odstavce 3 jsou **veřejnými listinami.**

Zákon 365/2000 Sb. §9 odst.4) **Osoba**, která je **držitelem prostředku pro elektronickou identifikaci**, který umožňuje přístup se zaručenou identitou, je oprávněna obstarat si s využitím tohoto prostředku **výstup** z informačního systému veřejné správy, který je neveřejnou evidencí, rejstříkem nebo seznamem,který se jí přímo týká. Správce portálu veřejné správy zveřejní na portálu veřejné správy informační systémy veřejné správy, z nichž lze výstup z informačního systému veřejné správy takto obstarat.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Poskytnutí údajů podle zákona 365/2000 Sb. §9 odst. 5)



Zákon 365/2000 Sb. §9 odst. 4) **Osoba**, která je držitelem **prostředku pro elektronickou identifikaci**, který umožňuje přístup se zaručenou identitou, je oprávněna obstarat si s využitím tohoto prostředku **výstup z informačního systému veřejné správy**, který je neveřejnou evidencí, rejstříkem nebo seznamem, který se jí přímo týká. Správce portálu veřejné správy zveřejní na portálu veřejné správy informační systémy veřejné správy, z nichž lze výstup z informačního systému veřejné správy takto obstarat.

Zákon 365/2000 Sb. §9 odst. 5) **Osoba**, která je držitelem **prostředku pro elektronickou identifikaci**, který umožňuje přístup se zaručenou identitou, je oprávněna umožnit s využitím tohoto prostředku poskytnutí výstupu z informačního systému veřejné správy podle odstavce 4, který se jí přímo týká, nebo **údajů vedených o ní** v informačním systému veřejné správy **jiné osobě anebo veřejnému orgánu.**

Osoba, která je držitel **prostředku pro elektronickou identifikaci** **nemá přímý přístup k údajům o ní vedených**, může jej však poskytnout jiným osobám anebo veřejnému orgánu dle §9 odst.5) poslední část věty.

Zpracování osobních údajů

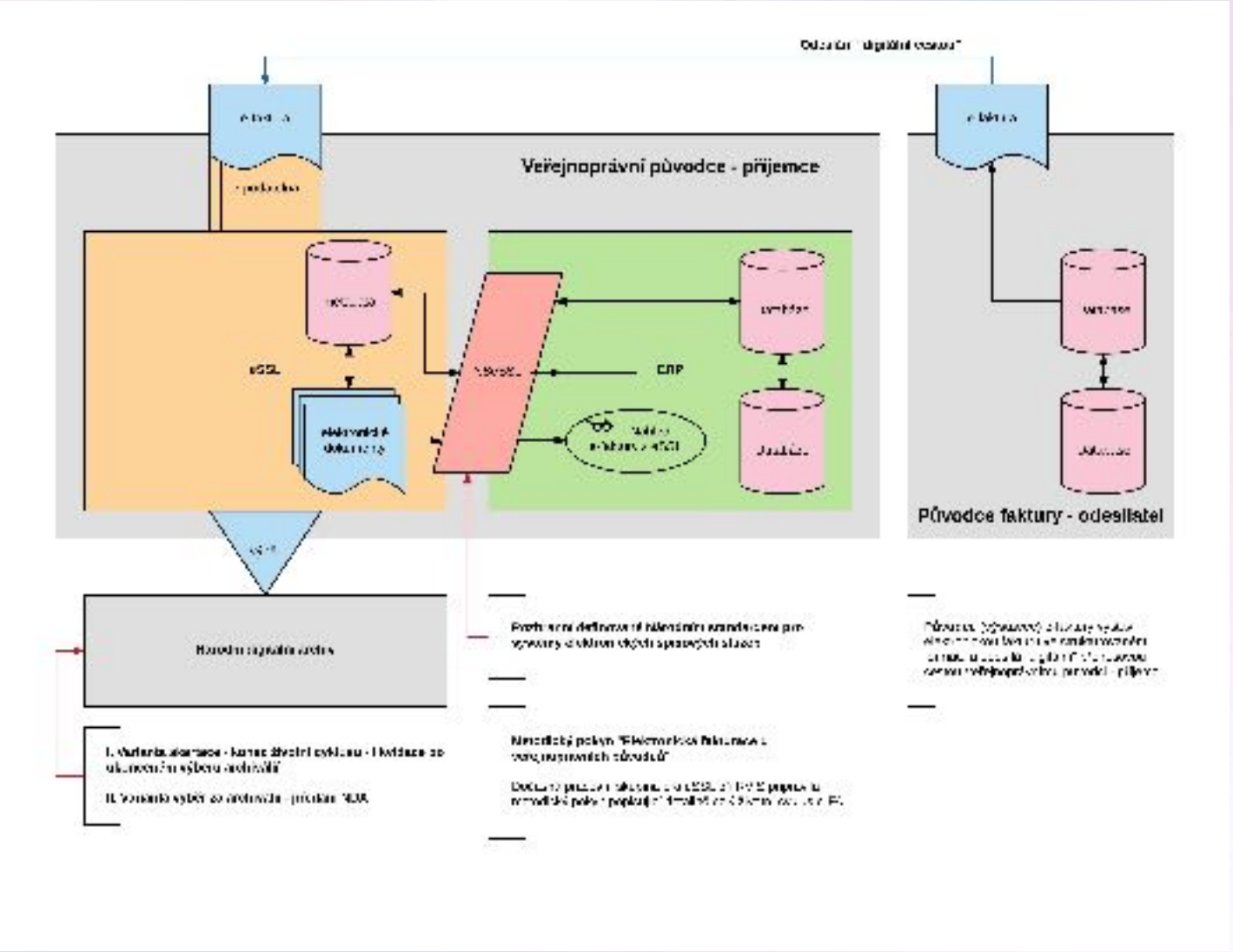
1. Správce osobních údajů "portálu občana" je Ministerstvo vnitra
2. Správce osobních údajů jsou dále pak veřejný orgán X a veřejných orgán Y
3. Zpracování je na základě aktivního **souhlasu držitele prostředku pro eID**, neboť údaje již jsou v některém z ISVS zpracovávány a podle §9 odst.5) jsou pouze poskytovány dalším osobám na základě souhlasu subjektu údajů

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příklad životního cyklu e-faktury u veřejnoprávních původců

E-FAKTURA

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



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

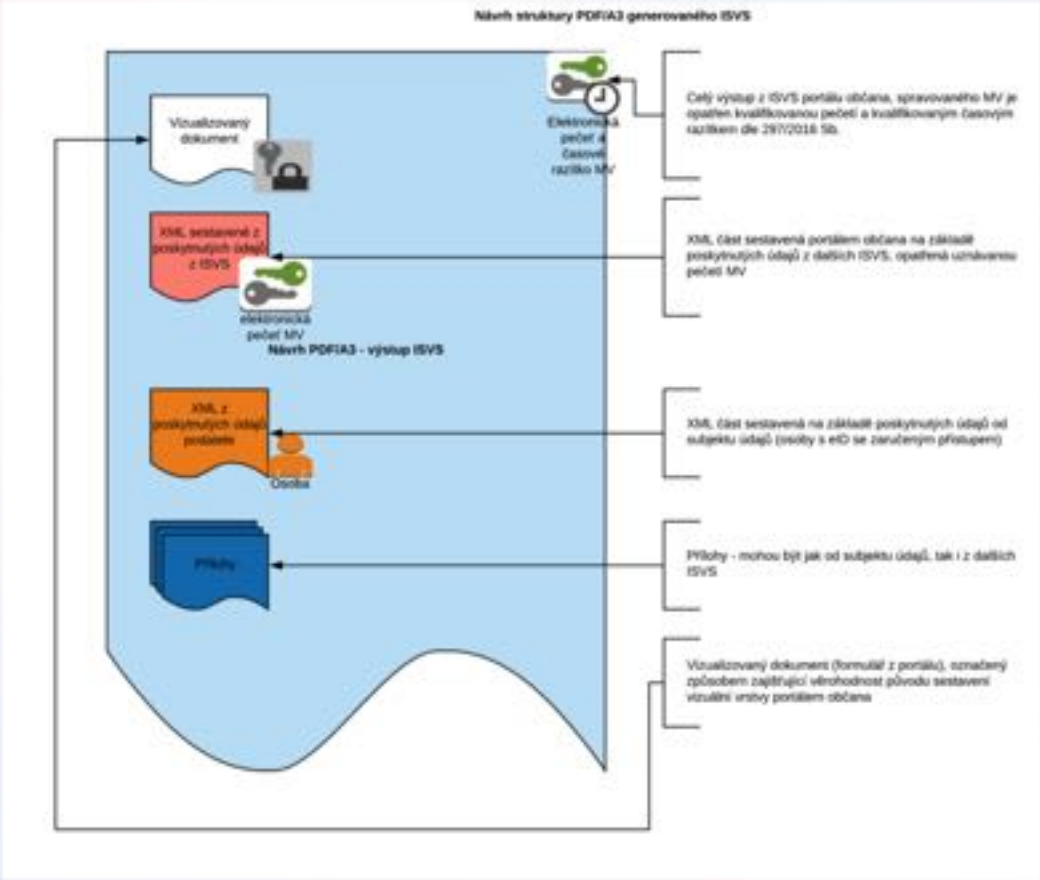
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

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

„inteligentní e-dokument“



MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

GDPR není REVOLUCE ale EVOLUCE!

DOPADY GDPR NA IT

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 omezení zpracování** dle článku 18
  - **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

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

Příklad dopadu nařízení GDPR na národní bod dle 250/2017 Sb.

PŘÍKLAD DOPADU GDPR NA NIA

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady GDPR na NIA

- 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

Příklad dopadu nařízení GDPR na elektronickou fakturaci

PŘÍKLAD DOPADU GDPR NA E-FA

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady GDPR na faktury

- 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

Příklad dopadu nařízení GDPR na eSSL

PŘÍKLAD DOPADU GDPR NA ESSL

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

eSSL a GDPR

- §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

Druhy dokumentů a dopady

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příklady dalších dopadů v souvislosti s IT

DALŠÍ DOPADY GDPR NA IT

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Dopady v souvislostech

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 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

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

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

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

Pomůcky pro kontrolu připravenosti a zavádění nových povinností

GDPR - CHECKLISTY

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

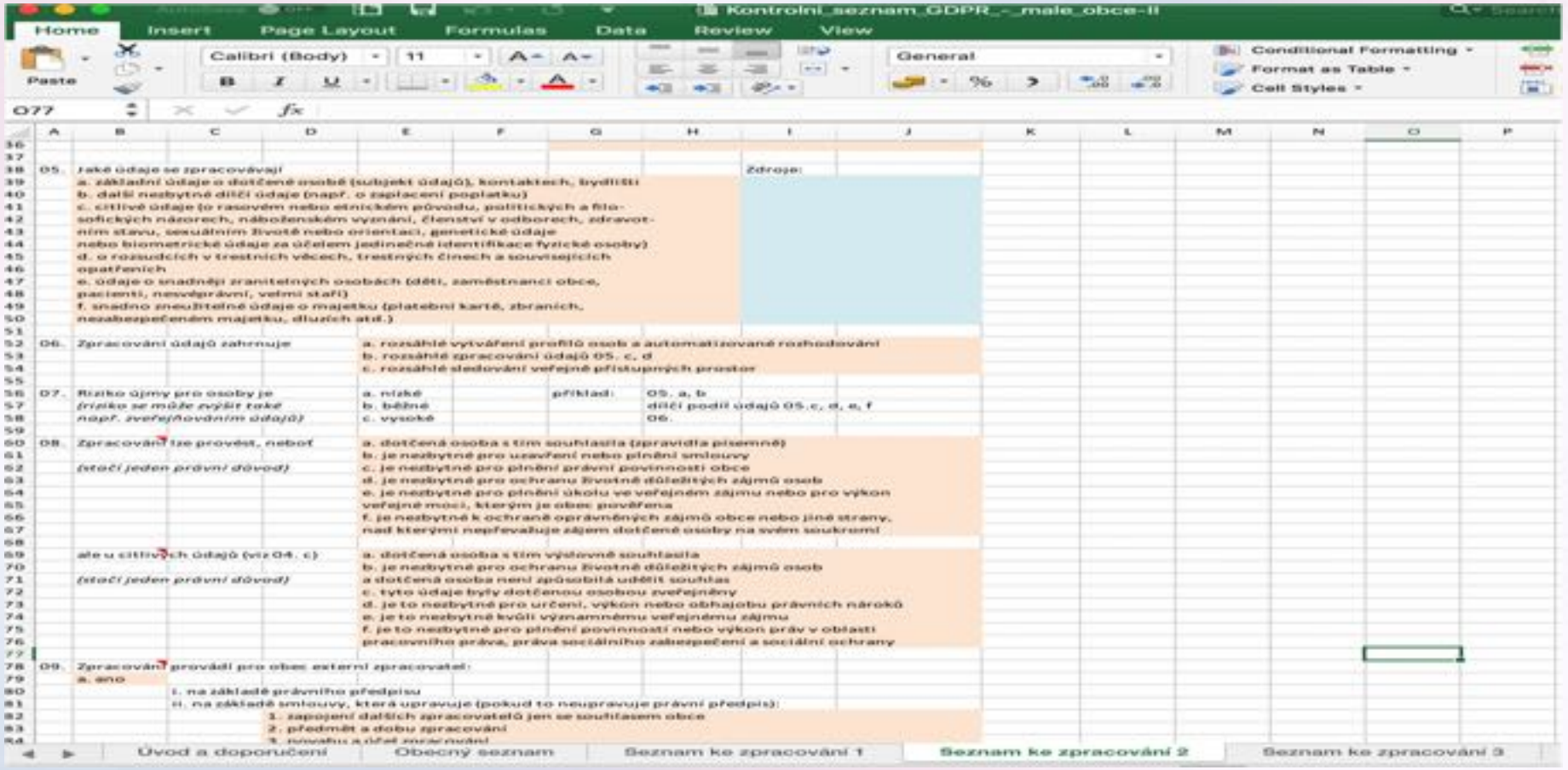
Checklisty pro obce

- Ministerstvo vnitra připravilo pro obce pomůcku pro rychlou kontrolu organizačního zabezpečení ochrany osobních údajů podle obecného nařízení o ochraně osobních údajů (GDPR)

- http://www.mvcr.cz/gdpr/clanek/gdpr-web-aktuality-aktuality-kontrolni-seznamy-checklisty-pro-obce.aspx

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

Příklad části checklistu



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 !