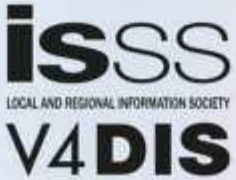
MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY



GDPR z pohledu ICT sekce MV

Ing.Robert Piffl

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

„Minulost je koulí na noze, kterou člověk vláčí za sebou.“

Zdeněk Chromý

ÚVOD

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL INFORMATION SOCIETY

Povinná četba

- 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 – dále jen „GDPR“)
- Materiály pracovní skupiny podle článku 29 směrnice 95/46/ES – nezávislý evropský poradní orgán
- Materiály ÚOOÚ – na webu jsou i překlady materiálů pracovní skupiny WP29 a některé poměrně zajímavé rozsudky (pro pochopení jak se na nařízení dívat)

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

„Čas je nehybný. Jenom my se v něm pohybujeme nesprávným směrem.“

Stanislaw Jerzy Lec

Už včera bylo pozdě …

KDY ZAČÍT

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
LOCAL AND REGIONAL INFORMATION SOCIETY
V4DIS

Nařízení GDPR - účinnost

- 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 má přednost před vnitrostátními právními předpisy - Nařízení na ochranu osobních údajů bude účinné od 25.5.2018 !**

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

GDPR aneb jak a kdy začít?

1. provedení „prvotního posouzení rizik“, tj. detailní analýza činnosti organizace s ohledem na charakter nařízení;
2. definice, které oblasti a v jakém rozsahu nařízení se organizace týkají;
3. úprava vnitřních procesů, směrnic, vzorů formulářů atd.;
4. úprava politiky ochrany osobních údajů;
5. úprava zpracovatelských smluv a smluv s dodavateli obecně;
6. zavedení procesu posuzování vlivu;
7. úprava veškerých informačních systémů takovým způsobem, aby byly v souladu s nařízením, a u vybraných zajištění novou funkcionalitu související například s právem na přenositelnost údajů, právem na výmaz a podobně;
8. zavedení postupů pro případy úniku osobních údajů;

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

Doporučené etapy “zavádění GDPR“ do praxe

DOPORUČENÝ POSTUP

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL INFORMATION SOCIETY

Doporučený postup – I.etapa

I. Etapa - provést úvodní školení a analýzy:

a) úvodní prezentace na téma GDPR pro vedoucí pracovníky, v případně i dalších organizací pokud jsou propojené;

b) školení na téma GDPR pro vedoucí jednotlivých dotčených úseků a případně i dalších organizací;

c) zmapování všech procesů relevantních z hlediska ochrany osobních údajů v rámci organizace a případně i dalších organizací;

d) právní analýza dopadů nařízení GDPR na činnost organizace a případně i dalších organizací.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

Doporučený postup – II.etapa

II. Etapa - identifikace změn:

a) podrobná analýza legislativních změn, které bude nutné či vhodné realizovat v souvislosti s přijetím nařízení a které budou spadat do gesce organizace (pokud je dotčená organizace místem odpovědným za tvorbu právních předpisů) a stručné vymezení změn, které bude nezbytné či vhodné v těchto předpisech učinit;

b) analýza souladu relevantních smluvních podmínek a smluvních vztahů, které mají trvat i po účinnosti nařízení, interních a externích procesů a interních a externích dokumentů;

c) návrh harmonogramu zohlednění GDPR ve smluvních vztazích (včetně připravovaných veřejných zakázek), procesech a dokumentech.

Doporučený postup – III.etapa

III. Implementace změn

a) návrh novel stávajících právních předpisů;

b) návrh compliance systému (příprava interních směrnic) organizace a případně i dalších souvisejících organizací pro oblast osobních údajů;

c) návrh úprav smluvních dokumentů, procesů a dokumentů organizace dle GDPR a vytvoření chybějící dokumentace;

d) monitoring vznikající národní legislativy a úprava navržených procesů a interních dokumentů dle závěrečné podoby národní legislativy;

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

Doporučený postup – III.etapa

III. Implementace změn

e) výkon funkce pověřence pro ochranu osobních údajů dle nařízení GDPR;

f) příprava manuálů pro zaměstnance v oblasti ochrany osobních údajů a související školení/workshop;

g) jednání s dodavateli organizace;

h) příprava a administrace zadávacích řízení na zajištění podpory procesů požadovaných nařízením v rámci činnosti organizace.

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL INFORMATION SOCIETY

Kontrolní bod k 2.4.2017

S ohledem na účinnost a rozsah dopadů nařízení GDPR by v současné době:

a. měla by být v organizacích dokončována II. etapa a měla by být zahajována III.etapa
b. mělo by být jasno ohledně výkonu funkce pověřence na ochranu osobních údajů (bude třeba nová pracovní pozice / stačí existující, atd..)
c. veškeré vznikající projekty by měly již být plně v souladu s nařízením GDPR s ohledem na jejich životní cyklus

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

ISSS
LOCAL AND REGIONAL
INFORMATION SOCIETY

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

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

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

Johann Wolfgang von Goethe

POVĚŘENEC

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL INFORMATION SOCIETY

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

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

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;
- Poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatňování podle článku 35;
- Spolupráce s dozorovým úřadem a
- 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

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

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

isss
LOCAL AND REGIONAL INFORMATION SOCIETY

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

isss
LOCAL AND REGIONAL INFORMATION SOCIETY

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

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

"Slibujeme pod vlivem nadějí a konáme pod vlivem strachu."

Francois de la Rochefoucauld

DOPADY NA IT

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL INFORMATION SOCIETY

Dopady / doporučení na IT

- Navrhnout změny v IT systémech
  - analyzovat dopady
  - harmonogram změn (prioritně od nejkritičtějších)
  - nezapomenout na „související formuláře“ a to nejen v listinné podobě (webové služby apod.)
  - pozor na nové funkcionality
    - právo na přenositelnost údajů
    - právo na opravu, právo na výmaz, …

MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

isss
LOCAL AND REGIONAL INFORMATION SOCIETY

Dopady / doporučení 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

isss
LOCAL AND REGIONAL
INFORMATION SOCIETY

„Jestliže četba nemá vliv na náš život, činy a myšlení, pak je škoda číst.“

Anton Pavlovič Čechov

ZÁVĚR

KONTAKT : ROBERT.PIFFL@MVCR.CZ