



# Adaptace GDPR

(Obecné nařízení o ochraně osobních údajů)  
v podmínkách působnosti  
resortu Ministerstva kultury ČR

Prezentaci připravila společnost F.S.C. Bezpečnostní poradenství

Přednášející: JUDr. Alena Kučerová

# Osnova

- Základní informace o novém právním rámci EU pro zpracování osobních údajů
- Co zůstává stejné a co se naopak změní
- Dopady GDPR do oblasti zpracování, které provádí resort kultury
- Jak dále???
- Otázky - odpovědi

# Základní informace o GDPR

- Bylo schváleno nové 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).
- Současně byla schválena nová Směrnice Evropského parlamentu a Rady (EU) 2016/680 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů příslušnými orgány za účelem prevence, vyšetřování, odhalování či stíhání trestných činů nebo výkonu trestů, o volném pohybu těchto údajů.

**Oba dokumenty jsou členské země EU povinny implementovat do konce května 2018!!!**

# Co zůstává stejné a co se naopak změní

**Obecné nařízení je přímo závazný právní předpis, který:**

**1. Ruší hmotně právní část zákona č. 101/2000 Sb.**

1. Dopad – připravuje se novelizace

**2. Ruší hmotně právní úpravu podmínek pro zpracování osobních údajů upravenou v řadě zvláštních předpisů**

1. Dopad - měla by se připravovat novelizace

**3. Zavádí jednotné pojmosloví, postupy, výklady, mechanismy**

1. Dopad – jednotnost v aplikaci

**4. Zavádí jednotné povinnosti správcům/zpracovatelům**

1. Dopad – snadnější vymahatelnost jejich dodržování

**5. Zavádí jednotná práva a prosazuje jejich uplatňování pro subjekty údajů**

1. Dopad – snadnější přístup k právu – jednotnost v aplikaci

# Co zůstává stejné?

## **1. Základní pojmosloví**

1. Ale přibyla řada nových pojmů

## **2. Zásady pro zpracování osobních údajů**

1. legalita a legitimita zpracování

## **3. Základní práva subjektu údajů**

1. Ale přibyla i nová oprávnění

## **4. Správce a zpracovatel**

1. Postavení, smluvní podmínky
2. Ale přibyla nové povinnosti

## **5. Předávání osobních údajů do třetích zemí**

1. Ale přibyla nová obecná pravidla

## **6. Nezávislý dozorový úřad**

# Co se změní – pro subjekt údajů?

## **Rozsah a forma informací, které je správce/zpracovatel povinen sdělovat subjektu údajů**

- Nyní se forma neupravuje vůbec a pokud jde o rozsah, je § 11 ZOOU poměrně stručný
- Příště správce bude muset poskytovat informace: stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků, zejména pokud jde o dítě; **do jednoho měsíce** od obdržení žádosti; s použitím standardizovaných a strojově čitelných ikon.

## **Rozsah oprávnění subjektu údajů**

- Nyní právo na přístup, na námitku a právo na informace
- Příště právo na přenositelnost údajů, právo být zapomenut...
- **Dnes si většinou řeší své záležitosti každý sám**
- **Příště:** Subjekt údajů má právo pověřit neziskový subjekt, organizaci nebo sdružení, jež vyvíjejí činnost v oblasti ochrany práv a svobod subjektů údajů, aby jeho jménem podal stížnost, uplatnil práva uvedená v článcích 77, 78 a 79. (čl. 80 Nařízení)

# Staronová práva subjektu údajů

- Dnes:
  - Právo na informaci (§ 11 ZOOU)
  - Právo na přístup (§ 12 ZOOU)
  - Právo na námitku (§ 21 ZOOU)
- GDPR:
  - Právo na informaci (čl. 13 a 14)
  - Právo na přístup (čl. 15)
  - Právo na opravu a výmaz = být zapomenut (čl. 16 a 17)
  - Právo na omezení zpracování (čl. 18)
  - Právo na přenositelnost (čl. 20)
  - Právo vznést námitku (čl. 21)

# Právo na přístup dnes a zítra

- § 12 Přístup subjektu údajů k informacím
  - Požádá-li subjekt údajů o informaci, je mu správce povinen tuto informaci bez zbytečného odkladu předat.
  - Obsahem informace je vždy sdělení o **účelu** zpracování, **osobních údajích**, případně kategoriích osobních údajů, které jsou předmětem zpracování, včetně veškerých dostupných informací o jejich **zdroji, povaze automatizovaného zpracování** v souvislosti s jeho využitím pro rozhodování, jestliže jsou na základě tohoto zpracování činěny úkony nebo rozhodnutí, jejichž obsahem je zásah do práva a oprávněných zájmů subjektu údajů, **příjemci**, případně kategoriích příjemců.



# Právo na přístup dnes a zítra

- Článek 15 **Právo subjektu údajů na přístup k osobním údajům**

- Subjekt údajů má právo získat od správce potvrzení, zda osobní údaje, které se ho týkají, jsou či nejsou zpracovávány, a pokud je tomu tak,
- má právo získat přístup:
  - k osobním údajům
  - k následujícím informacím:
    - **účely** zpracování; **kategorie** dotčených osobních údajů; **příjemci** nebo kategorie příjemců, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích; **plánovaná doba**, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritéria použitá ke stanovení této doby;
    - **existence práva** požadovat od správce opravu nebo výmaz osobních údajů nebo omezení jejich zpracování a nebo vznést námitku proti tomuto zpracování; právo podat stížnost u dozorového úřadu;
    - informace o **zdroji** osobních údajů, pokud nejsou získány od subjektu údajů;
    - skutečnost, že dochází k automatizovanému rozhodování, včetně profilování, a přinejmenším v těchto případech smysluplné informace týkající se použitého postupu, jakož i významu a předpokládaných důsledků takového zpracování pro subjekt údajů.
- Pokud se osobní údaje předávají do třetí země nebo mezinárodní organizaci, má subjekt údajů právo být informován o vhodných zárukách podle článku 46, které se vztahují na předání.
- Správce poskytne kopii zpracovávaných osobních údajů. Jestliže subjekt údajů podává žádost v elektronické formě, poskytnou se informace v elektronické formě, která se běžně používá, pokud subjekt údajů nepožádá o jiný způsob.
- Právem získat kopii nesmějí být nepříznivě dotčena práva a svobody jiných osob.

# Právo vznést námitku dnes a zítra

- **§ 21 Ochrana práv subjektů údajů**

- Každý subjekt údajů, který zjistí nebo se domnívá, že správce nebo zpracovatel provádí zpracování jeho osobních údajů, které je v rozporu s ochranou soukromého a osobního života subjektu údajů nebo v rozporu se zákonem, zejména jsou-li osobní údaje nepřesné s ohledem na účel jejich zpracování, může
  - **požádat** správce nebo zpracovatele **o vysvětlení,**
  - **požadovat,** aby správce nebo zpracovatel **odstranil takto vzniklý stav.** Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.
- Je-li žádost subjektu údajů shledána oprávněnou, správce nebo zpracovatel odstraní neprodleně závadný stav.

# Právo vznést námitku dnes a zítra

- **Článek 21 Právo vznést námitku**

- Subjekt údajů má **právo kdykoli vznést námitku** proti zpracování osobních údajů, které se jej týkají, na základě čl. 6 odst. 1 písm. e) nebo f), včetně profilování.
  - zpracování je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci;
  - zpracování je nezbytné pro účely oprávněných zájmů správce či třetí strany, kromě případů, kdy před těmito zájmy mají přednost zájmy nebo základní práva a svobody subjektu údajů vyžadující ochranu osobních údajů, zejména pokud je subjektem údajů dítě.
- **Správce osobní údaje dále nezpracovává, pokud neprokáže závažné oprávněné důvody** pro zpracování, které převažují nad zájmy nebo právy a svobodami subjektu údajů, nebo pro určení, výkon nebo obhajobu právních nároků.
- Pokud se osobní údaje zpracovávají pro **účely přímého marketingu**, má subjekt údajů právo vznést kdykoli námitku proti zpracování údajů, které se ho týkají, pro tento marketing, což zahrnuje i profilování.
  - Pokud subjekt údajů vznesl námitku proti zpracování pro účely přímého marketingu, nebudou již osobní údaje pro tyto účely zpracovávány.
- **Subjekt údajů je na právo uvedené v odstavcích 1 a 2 výslovně upozorněn** a toto právo je uvedeno zřetelně a odděleně od jakýchkoli jiných informací, a to nejpozději v okamžiku první komunikace se subjektem údajů.
  - V souvislosti s využíváním služeb informační společnosti, a aniž je dotčena směrnice 2002/58/ES, může subjekt údajů uplatnit své právo vznést námitku automatizovanými prostředky pomocí technických specifikací.
- Jsou-li osobní údaje zpracovávány pro účely vědeckého či historického výzkumu nebo pro statistické účely podle čl. 89 odst. 1, má subjekt údajů, z důvodů týkajících se jeho konkrétní situace, právo vznést námitku proti zpracování osobních údajů, které se ho týkají, ledaže je zpracování nezbytné pro splnění úkolu prováděného z důvodů veřejného zájmu.

# Článek 20 Právo na přenositelnost údajů

- Subjekt údajů má **právo získat osobní údaje**, které se ho týkají, jež poskytl správci, ve strukturovaném, běžně používaném a strojově čitelném formátu, a právo předat tyto údaje jinému správci, aniž by tomu správce, kterému byly osobní údaje poskytnuty, bránil, a to v případě, že:
  - **zpracování je založeno na souhlasu** podle čl. 6 odst. 1 písm. a) nebo čl. 9 odst. 2 písm. a) **nebo na smlouvě** podle čl. 6 odst. 1 písm. b);
  - zpracování se provádí automatizovaně.
- Při výkonu svého práva má subjekt údajů právo na to, aby osobní údaje byly předány přímo jedním správcem správci druhému, je-li to technicky proveditelné.
- Výkonem práva není dotčen článek 17 (právo na výmaz).
- **Toto právo se neuplatní** na zpracování nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen.
- Právem uvedeným v odstavci 1 nesmí být nepříznivě dotčena práva a svobody jiných osob.

# Co se změní pro správce/zpracovatele?

## Rozsah dokumentační povinnosti – smlouva o zpracování

- Dnes povinnost podle § 6 ZOOU – náležitosti smlouvy - záruky
- Příště povinnosti podle čl. 28 Nařízení – náročnost

## Rozsah dokumentační povinnosti – technicko-organizační opatření

- Dnes obsah a rozsah TOO dle § 13 ZOOU - zabezpečení
- Příště: soulad s čl. 24 odst. 1 Nařízení:
  - Správce zavede vhodná technická a organizační opatření k zajištění toho, aby se:
  - standardně zpracovávaly pouze osobní údaje, jež jsou pro každý konkrétní účel daného zpracování nezbytné.
  - Tato povinnost se týká **množství** shromážděných osobních údajů, **rozsahu** jejich zpracování, **doby** jejich uložení a jejich **dostupnosti**. (čl. 25 Nařízení)

# Co se změní pro správce/zpracovatele?

## **1. Vedení záznamů o činnostech zpracování (čl. 30)**

- Netýká se sice malých organizací, ale....

## **2. Provádět ohlašování případů porušení zabezpečení osobních údajů UOOU/subjektu údajů (čl. 33 a 34)**

- Týká se každého povinného subjektu

## **3. Provádět posouzení vlivu na ochranu osobních údajů a povinnost předchozí konzultace (čl. 35 a 36)**

- Netýká se všech, ale ....

## **4. Ustanovit pověřence pro ochranu osobních údajů (čl. 37)**

- Ve státním sektoru musí všichni
- V soukromém sektoru musí jen někteří, ale...

# Proč jsme se sešli?

- **Obecné nařízení o ochraně osobních údajů 2016/679**

- Platné od 25. května 2016/Účinné od 25. května 2018;
- Je přímo závazným právním předpisem, který musí být aplikován v celém rozsahu;
- Dopadá jak na zákon č. 101/2000 Sb., tak na všechny zvláštní právní předpisy, které upravují podmínky pro zpracování osobních údajů v oblasti, kterou představuje:
  - UMĚNÍ, KNIŽNÍ KULTURA A KNIHOVNY
  - STÁTNÍ PAMÁTKOVÁ PÉČE
  - OCHRANA MOVITÉHO KULTURNÍHO DĚDICTVÍ, MUZEA A GALERIE
  - HROMADNÉ SDĚLOVACÍ PROSTŘEDKY A KINEMATOGRAFIE
  - PROVÁDĚNÍ AUTORSKÉHO ZÁKONA
  - CÍRKVE A NÁBOŽENSKÉ SPOLEČNOSTI

# K jednotlivým novým povinnostem

## Článek 30 Nařízení - **Záznamy o činnostech zpracování:**

1. Každý správce a jeho případný zástupce vede záznamy o činnostech zpracování, za něž odpovídá.
2. Tyto záznamy obsahují taxativně vymezený rozsah informací.
3. Stejnou povinnost má i zpracovatel.
4. Záznamy podle odstavců se vyhotovují písemně, v to počítaje i elektronickou formu.
5. Správce, zpracovatel nebo případný zástupce správce nebo zpracovatele poskytne záznamy na požádání dozorového úřadu.
6. **Výjimka** pro podnik nebo organizaci zaměstnávající **méně než 250 osob**, ale pokud
  1. **zpracování, které provádí, pravděpodobně představuje riziko** pro práva a svobody subjektů údajů,
  2. zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

**Závěr: Bude se vztahovat i na resort MK**



# K jednotlivým novým povinnostem

## Článek 33 Nařízení - **Ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu**

- 1. Jakékoli porušení zabezpečení osobních údajů** správce bez zbytečného odkladu a pokud možno do 72 hodin od okamžiku, kdy se o něm dozvěděl, ohlásí dozorovému úřadu příslušnému podle článku 55, ledaže je nepravděpodobné, že by toto porušení mělo za následek riziko pro práva a svobody fyzických osob.
2. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.
3. Jakmile zpracovatel zjistí porušení zabezpečení osobních údajů, ohlásí je bez zbytečného odkladu správci.

## Článek 34 Nařízení - **Oznamování případů porušení zabezpečení osobních údajů subjektu údajů**

**Závěr: Bude se vztahovat i na resort MK**

# K jednotlivým novým povinnostem

## Článek 35 Nařízení - **Posouzení vlivu na ochranu osobních údajů - DPIA**

1. Pokud je pravděpodobné, že určitý **druh zpracování**, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování **bude mít za následek vysoké riziko** pro práva a svobody fyzických osob, **provede správce před zpracováním** posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů.
2. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.
3. Posouzení vlivu je nutné zejména v těchto případech:
  1. systematické a rozsáhlé vyhodnocování osobních aspektů týkajících se fyzických osob, které je založeno na automatizovaném zpracování, včetně profilování, a na němž se zakládají rozhodnutí,
  2. rozsáhlé zpracování zvláštních kategorií údajů nebo osobních údajů týkajících se rozsudků v trestních věcech a trestných činů,
  3. **rozsáhlé systematické monitorování veřejně přístupných prostorů.**

Dozorový úřad sestaví a zveřejní seznam druhů operací zpracování, které podléhají požadavku na posouzení vlivu

**Závěr: Bude se vztahovat i na resort MK**

# K jednotlivým novým povinnostem

- Článek 37 Nařízení - **Jmenování pověřence pro ochranu osobních údajů**

1. Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:
  1. zpracování provádí **orgán veřejné moci či veřejný subjekt**, s výjimkou soudů jednajících v rámci svých soudních pravomocí;
  2. **hlavní činnosti** správce nebo zpracovatele spočívají v operacích zpracování, které kvůli své povaze, svému rozsahu nebo svým účelům vyžadují **rozsáhlé pravidelné a systematické monitorování** subjektů údajů;
  3. hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.
2. Skupina podniků může jmenovat jediného pověřence pro ochranu osobních údajů, pokud je snadno dosažitelný.
3. Pověřenec může být pracovníkem správce či zpracovatele, nebo může úkoly plnit na základě smlouvy o poskytování služeb.

**Závěr: Bude se vztahovat na ministerstvo, v dalších případech bude třeba dopad analyzovat.**

# Požadavky na zabezpečení osobních údajů

- Článek 32 **Zabezpečení zpracování**

- S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:
  - pseudonymizace a šifrování osobních údajů;
  - schopnosti zajistit neustálou **důvěrnost, integritu, dostupnost a odolnost systémů a služeb** zpracování;
  - schopnosti obnovit dostupnost osobních údajů a přístup k nim včas v případě fyzických či technických incidentů;
  - procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.
- Při posuzování vhodné úrovně bezpečnosti se zohlední zejména rizika, která představuje zpracování, zejména náhodné nebo protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění předávaných, uložených nebo jinak zpracovávaných osobních údajů, nebo neoprávněný přístup k nim.
- Jedním z prvků, jimiž lze doložit soulad s požadavky stanovenými v tomto článku, je
  - dodržování schváleného kodexu chování uvedeného v článku 40
  - uplatňování schváleného mechanismu pro vydávání osvědčení uvedeného v článku 42.

# Nějaké další otázky?

- Prosím, ptejte se!!!!



Děkuji za Vaši pozornost

JUDr. Alena Kučerová

Ředitelka útvaru ochrany informací společnosti