Co nového do ochrany osobních údajů přináší nařízení 2016/679

Naposledy upraveno 7. listopadu 2017

PhDr. Miroslava Matoušová

úřad pro ochranu osobních údajů
the office for personal data protection

- **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)**
- **Účinnost („*použije se od*“): 25. května 2018**

- **Směrnice EP 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 a o zrušení rámcového rozh. Rady 2008/977/SVV**
- **Provedení ve vnitrostátním právu od 6. května 2018**

úřad pro ochranu osobních údajů
the office for personal data protection

Část I

ZÁSADY OCHRANY OSOBNÍCH ÚDAJŮ A ZÁSADY ZPRACOVÁNÍ

úřad pro ochranu osobních údajů
the office for personal data protection

Obecná charakteristika

- Kontinuita (zásady a klíčové instrumenty)
- Promítnutí vývoje informačních technologií pro zpracování osobních údajů a globalizace
- Prováděcí unijní i vnitrostátní předpisy, omezení rozsahu povinností/práv předpisy

Zásady ochrany osobních údajů

- Práva subjektů údajů
- Povinnosti správců a zpracovatelů
- Záměrná a standardní ochrana
- Přístup založený na riziku
- Panevropský (EU) dosah
- Nezávislý dozor
- Vymahatelnost

úřad pro ochranu osobních údajů
the office for personal data protection

Zásady zpracování os. údajů: čl. 5 obecného nařízení

- zákonnost, korektnost a transparentnost ve vztahu k subjektu údajů
- účelové omezení
- minimalizace údajů
- přesnost (os. údajů)
- omezení uložení
- integrita a důvěrnost
- odpovědnost (správce)

úřad pro ochranu osobních údajů
the office for personal data protection

Transparentnost jako zásada

- Článek 5(1): *Osobní údaje musí být:*
- *a) ve vztahu k subjektu údajů zpracovány korektně a zákonným a transparentním způsobem („zákonnost, korektnost a transparentnost“)*
- Za její porušení lze uložit správní pokutu až do výše 20 000 000 EUR, nebo 4% celkového ročního obratu celosvětově za předchozí finanční rok
- Navázána na novou zásadu odpovědnosti: podle čl. 5(2) správce odpovídá za dodržení zásady transparentnosti a musí být schopen dodržení souladu doložit.

úřad pro ochranu osobních údajů
the office for personal data protection

Transparentnost jako zásada 2

- Překlenovací povinnost promítnutá v:
  - Poskytování informací vztahujících se ke korektnímu zpracování subjektům údajů,
  - Komunikaci správců se subjekty údajů o jejich právech z ON,
  - Usnadňování výkonu práv subjektů údajů.

úřad pro ochranu osobních údajů
the office for personal data protection

Zásada odpovědnosti

- Správce odpovídá za dodržení všech zásad a musí být schopen dodržení doložit
- Dodržování nutno prokazovat aktivně
- Provedení zásady v řadě článků jako součást specifických povinností
- Sankční odpovědnost (správní pokuty, čl. 83)
- Odpovědnost za újmu způsobenou zpracová-ním, jež porušuje ON (čl. 82) x právo na náhradu újmy

úřad pro ochranu osobních údajů
the office for personal data protection

Zásady zpracování os. údajů: čl. 5 obecného nařízení

- zákonnost, korektnost a transparentnost ve vztahu k subjektu údajů x hl. II a III zák. č.101/2000 Sb.
- účelové omezení x § 5 odst. 1 písm. a), d) a f) dto
- minimalizace údajů x § 5 odst. 1 písm. d)
- přesnost (os. údajů) x § 5 odst. 1 písm. c)
- omezení uložení x § 5 odst. 1 písm. e)
- integrita a důvěrnost x § 13
- odpovědnost (správce)

úřad pro ochranu osobních údajů
the office for personal data protection

Nová definice příjemce

- fyzická nebo právnická osoba, orgán veřejné moci, agentura nebo jiný subjekt, kterým jsou osobní údaje poskytnuty, ať už se jedná o třetí stranu, či nikoli
- orgány veřejné moci, které mohou získávat osobní údaje v rámci zvláštního šetření v souladu s právem ČS, se za příjemce nepovažují; zpracování těchto osobních údajů těmito orgány veřejné moci musí být v souladu s použitelnými pravidly pro ochranu údajů v souladu s účely zpracování

úřad pro ochranu osobních údajů
the office for personal data protection

Politické x odborné čtení ON

úřad pro ochranu osobních údajů
the office for personal data protection

Definice osobního údaje

- omezení na údaje identifikující
- rozšíření pojmu

- Definice v § 4 zák. č. 101/2000 Sb., čl. 2 směrnice 95/46/ES a čl. 4 ON
- rozsudky Breyer (C-582/14) a Scarlet Extended SA (C-70/10)
- rozsudky Schrems (C-362/14), Tele2Sverige (C-203/15), Tele2/Watson (C-698/15) …

úřad pro ochranu osobních údajů
the office for personal data protection

Ochrana cestuje s osobními údaji

- V celé Unii je třeba zajistit soudržné a jednotné uplatňování pravidel ochrany

  -preambule (10)

- Podmínky zákonnosti zpracování: možnost ČS zavést konkrétnější ust. podle čl. 6(1)c) a e)
- Omezení rozsahu povinností a práv podle čl. 5,12-22 a 34 právem Unie/ČS (čl. 23)
- Právo ČS uvádějící právo na ochranu os. údajů podle ON do souladu s právem na svobodu projevu a informací (čl. 85)

úřad pro ochranu osobních údajů
the office for personal data protection

Část II

Konstrukční základy a nové instituty ochrany osobních údajů

úřad pro ochranu osobních údajů
the office for personal data protection

Nové nástroje ochrany

- pověřenec pro ochranu osobních údajů
- ohlašování případů porušení zabezpečení osobních údajů dozorovému úřadu a oznamování téhož dotčeným subjektům údajů
- mechanismus jediného kontaktního místa
- mechanismus jednotnosti (ON) a vzájemná pomoc dozorových úřadů, vč. úkolů sboru (sm)

úřad pro ochranu osobních údajů
the office for personal data protection

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.

Záměrná a standardní ochrana 2

- 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)

Záměrná a standardní ochrana 3

- 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

úřad pro ochranu osobních údajů
the office for personal data protection

Záměrná a standardní ochrana a transparentnost

- Kodexy chování (dodržování schváleného kodexu chování)

- Osvědčení o ochraně osobních údajů, pečetě a známky (dodržování schváleného mechanismu pro vydávání osvědčení)

úřad pro ochranu osobních údajů
the office for personal data protection

Přístup založený na riziku

- Klíčem k nastavování povinností pro správce je rizikovost, která je samozřejmě dovozována z rozsahu zpracování, zpracovávaných osobních údajů (citlivé údaje)a používaných technologií.

úřad pro ochranu osobních údajů
the office for personal data protection

Přístup založený na riziku: **zabezpečení zpracování** 2

- 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 s 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.
- Při posuzování úrovně bezpečnosti se zohlední zejm. rizika ze zpracování (náhodné/protiprávní zničení, ztráta, pozměňování, neoprávněné zpřístupnění osobních údajů, neoprávněný přístup).

úřad pro ochranu osobních údajů
the office for personal data protection

Přístup založený na riziku: **ohlašování a oznamování porušení zabezpečení os.údajů** 3

• Porušení zabezpečení ohlásí správce bez zbytečného odkladu a pokud možno do 72 hod. od okamžiku, kdy se o něm dozvěděl, dozorovému úřadu, ledaže je nepravděpodobné, že by mělo za následek riziko pro práva a svobody fyzických osob.

• Pokud je pravděpodobné, že porušení bude mít za následek vysoké riziko /…/, oznámí správce porušení bez zbytečného odkladu subjektu údajů. Oznámení se nevyžaduje, jestliže:

a) náležitá technická a organizační ochranná opatření byla použita u údajů dotčených porušením, zejm. ta, která činí údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, např. šifrování;

b) správce přijal následná opatření, která zajistí, že vysoké riziko /…/ se již pravděpodobně neprojeví.

úřad pro ochranu osobních údajů
the office for personal data protection

Přístup založený na riziku: Posouzení vlivu 4

- Pokud je pravděpodobné, že určitý druh zpracování, zejm. při využití nových technologií, bude mít s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování za následek vysoké riziko pro práva a svobody, provede správce posouzení vlivu zamýšlených operací na ochranu osobních údajů.
- Posouzení je nutné zejména v těchto případech:

a)systematické a rozsáhlé vyhodnocování osobních aspektů fyzických osob, které je založeno na automatizovaném zpracování, vč. profilování, a na němž se zakládají rozhodnutí s právními účinky nebo mají na fyzické osoby podobně závažný dopad;

b) rozsáhlé zpracování zvláštních kategorií údajů (citlivé) nebo údajů týkajících se rozsudků v trestních věcech a trestných činů;

c) rozsáhlé systematické monitorování veřejně přístupných prostorů.

Přístup založený na riziku: Předchozí konzultace 5

- Správce konzultuje před zpracováním s dozorovým úřadem, pokud z posouzení vlivu na ochranu osobních údajů vyplývá, že by dané zpracování mělo za následek vysoké riziko v případě, že by správce nepřijal opatření ke zmírnění tohoto rizika.
- Pokud se dozorový úřad domnívá, že by zamýšlené zpracování porušilo toto nařízení, zejména pokud správce nedostatečně určil či zmírnil riziko, upozorní na to správce a případně zpracovatele údajů písemně ve lhůtě nejvýše osmi týdnů od obdržení žádosti o konzultaci a může uplatnit kteroukoli ze svých pravomocí.

úřad pro ochranu osobních údajů
the office for personal data protection

Přístup založený na riziku: Pověřenec pro ochranu osobních údajů 6

Správce a zpracovatel jmenují pověřence pro ochranu osobních údajů v každém případě, kdy:

a) zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí;

b) 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;

c) hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů a osobních údajů týkajících se rozsudků v trestních věcech a trestných činů.

Přístup založený na riziku: **Předávání do třetích zemí a mezinárodním organizacím** 7

- 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 a týkají se pouze omezeného počtu subjektů údajů, lze uskutečnit pro účely závažných oprávněných zájmů správce, pokud nad těmito zájmy nepřevažují zájmy/práva a svobody subjektu údajů

úřad pro ochranu osobních údajů
the office for personal data protection

Přístup založený na riziku: pseudonymizace 8

- 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

Sjednocený dozor nad ochranou osobních údajů

úřad pro ochranu osobních údajů
the office for personal data protection

Sjednocení dozoru

- Upravena nezávislost, podmínky pro členy, úkoly a pravomoci (vč. vyšetřovacích) dozorových úřadů a vzájemná spolupráce dozorových úřadů
- Evropský sbor pro ochranu osobních údajů jako subjekt Unie s právní subjektivitou k dosahování jednotnosti v prosazování a vymáhání pravidel (mechanismus jednotnosti) x podpora soudržného uplatňování směrnice
- Jednotné sankce (podmínky ukládání správních pokut s horní hranicí 20 mil. EUR, nebo - pouze u podniků - 4% ročního obratu za předchozí finanční rok)
- Mechanismus jednotnosti (ON) x spolupráce dozorových úřadů (směrnice)

úřad pro ochranu osobních údajů
the office for personal data protection

Mechanismus jediného kontaktního místa

- Každý subjekt údajů by měl mít právo podat stížnost u jediného dozorovému úřadu, zejména v členském státě, kde má své obvyklé bydliště
- ČS, který zřídil více dozorových úřadů, by měl určit úřad, který bude fungovat jako jediné kontaktní místo v mechanismu
- Nevztahuje se na zpracování prováděné orgány veřejné moci nebo soukromé subjekty ve veřejném zájmu

úřad pro ochranu osobních údajů
the office for personal data protection

Mechanismus jednotnosti: úkol a nástroje

- Dozorové úřady spolupracují mezi sebou navzájem a ve vhodných případech s Komisí prostřednictvím mechanismu jednotnosti

- Stanovisko sboru (ON)
- Řešení sporů sborem
- Postup pro naléhavé případy
- Výměna informací (KOM)

úřad pro ochranu osobních údajů
the office for personal data protection

Mechanismus jednotnosti: sjednocující nástroje na úrovni EU

- Pokyny, doporučení a osvědčené postupy
- Schvalování kritérií pro vydávání osvědčení
- Stanoviska k návrhům rozhodnutí dozorových úřadů
- Závazná rozhodnutí ve sporech
- Poradenství (adresované) Komisi
- Veřejné registry rozhodnutí dozorových úřadů a soudů k otázkám řešeným mechanismem jednotnosti a mechanismů pro vydávání osvědčení

úřad pro ochranu osobních údajů
the office for personal data protection

Část III

Práva subjektu údajů

Subjekt údajů má kontrolu nad svými údaji

- Subjektu údajů se nově přiznává kontrola nad svými údaji
- Subjekt údajů je (výlučným) vlastníkem svých osobních údajů
  - (privátní autonomie)
- Souhlas pouze jedním ze 6 právních titulů
- Rozšířená práva: přenositelnost
- Detailnější úprava (výmaz)
- Omezení práv:
  - v samotném ON
  - přípustné právem Unie/ČS (čl. 23)

úřad pro ochranu osobních údajů
the office for personal data protection

Práva subjektu údajů

- Právo na informace od správce
- Právo na přístup k osobním údajům
- Právo na opravu
- Právo na výmaz („být zapomenut“)
- Právo na omezení zpracování
- Právo na přenositelnost údajů
- Právo vznést námitku
- Právo nebýt předmětem automatizovaného rozhodování

úřad pro ochranu osobních údajů
the office for personal data protection

Právo být zapomenut

- „Na pravou míru“ uvedeno přímo v ON:
  - *Čl. 17 Právo na výmaz („právo být zapomenut“) pokud je dán jeden ze 6 důvodů*
  - *Nepoužije se, při zpracování nezbytném pro jeden ze 4 důvodů (výkon práva na svobodu projevu a informace, splnění právní povinnosti, veřejného zájmu v oblasti veřejného zdraví, pro účely archivace ve veř. zájmu, vědeckého/historického výzkumu nebo statistické účely a pro určení, výkon nebo obhajobu právních nároků)*

úřad pro ochranu osobních údajů
the office for personal data protection

Práva subjektu údajů: zastupování

Subjekt údajů má právo pověřit neziskový subjekt, organizaci nebo sdružení, jež byly založeny v souladu s právem některého ČS, jejichž statutární cíle jsou ve veřejném zájmu a jež jsou činné v oblasti práv a svobod subjektů údajů ohledně ochrany jejich osobních údajů, aby jeho jménem podal stížnost a uplatnil práva podat stížnost u dozorových úřadů, právo na účinnou soudní ochranu vůči dozorovému úřadu a správci/zpracovateli

úřad pro ochranu osobních údajů
the office for personal data protection

Souhlas subjektu údajů

1

- zásadní institut evropského modelu ochrany osobních údajů
- svobodnost: plnění smlouvy, vč. poskytnutí služby nesmí být podmíněno souhlasem se zpracováním, které není pro plnění dané smlouvy nutné
- Specifičnost: získáván k jednomu nebo několika účelům
- Odvolatelnost (standardizovaný a dostupný postup)
- nevyužit přístup založený na riziku

Transparentnost a souhlas subjektu údajů 2

- Oddělitelnost, samostatnost
- Srozumitelnost
- „samostatně“ pro různé účely
- žádost o vyjádření souhlasu jasně odlišena od jiných skutečností, snadno přístupná
- jasné a jednoduché jazykové prostředky
- vrstvený souhlas

úřad pro ochranu osobních údajů
the office for personal data protection

Povinnosti správců naplňující práva subjektů údajů: čl. 12 - 21

- Povinný obsah
- Časové určení okamžiku plnění (lhůta)
- Výjimky z povinnosti poskytnout informace, pokud a v míře, v níž subjekt údajů informace má
- Doplnění informací podle čl. 13 a 14 standardizovanými ikonami
- Povinnost správce poskytnout kopii osobních údajů (čl. 15)

úřad pro ochranu osobních údajů
the office for personal data protection

Část IV aneb S čím správcům pomůže komunita ochránců?

METODICKÉ DOKUMENTY WP29

úřad pro ochranu osobních údajů
the office for personal data protection

Vodítka: vydaná

1

- *První a druhé vydání:*
- Pověřenec pro ochranu osobních údajů (wp243rev.01)
- Přenositelnost osobních údajů (wp242rev.01)
- Určení vedoucího dozorového úřadu pro správce nebo zpracovatele (wp244rev.01)
- Posouzení vlivu na ochranu osobních údajů a zjišťování, zda zpracování „bude mít za následek vysoké riziko“pro účely ON (wp248rev.01)
- *První vydání: (veřejná konzultace do 28. listopadu 2017)*
- Automatizované individuální rozhodování a profilování pro účely nařízení (wp251)

úřad pro ochranu osobních údajů
the office for personal data protection

Vodítka: vydaná

2

- *První vydání: (bez veřejné konzultace)*
- správní pokuty (wp253)

úřad pro ochranu osobních údajů
the office for personal data protection

Vodítka: připravovaná

- vydávání osvědčení (certifikace)
- souhlas subjektu údajů
- transparentnost
- předávání osobních údajů
- Interní EDPB: mezinárodní spolupráce, postup v naléhavých případech

úřad pro ochranu osobních údajů
the office for personal data protection

www.uoou.cz

https://www.uoou.cz/obecne-narizeni-eu/ds-3938/p1=3938

úřad pro ochranu osobních údajů
the office for personal data protection