

Ochrana osobních údajů

Kateřina Krčálová Konečná

katerina.krcalova@gmail.com

Legislativa

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) – **obecné nařízení GDPR**

- ochrana fyzických osob v souvislosti se zpracováním jejich osobních údajů (OÚ) je jejich **základním právem**
- Listina základních práv EU a Smlouva o fungování EU přiznávají každému právo na ochranu OÚ
- účelem nařízení GDPR je harmonizovat zpracování OÚ v jednotlivých čl. státech EU a zajistit volný pohyb OÚ mezi čl. státy
- nařízení obsahuje v úvodu rozsáhlé zdůvodnění právní úpravy

čl. 1 Předmět a cíle

- pravidla ochrany fyzických osob (FO) v souvislosti se zpracováním OÚ a pravidla týkající se volného pohybu OÚ
- volný pohyb OÚ není v EU omezen ani zakázán (ale musí podléhat stanoveným pravidlům)
- při předání OÚ mimo území EU jsou stanoveny dodatečné podmínky (čl. 44 - čl. 50)
- nařízení se vztahuje jen na fyzické osoby, nedopadá na OÚ právnických osob
- nařízení se nevztahuje na OÚ zesnulých osob (řeší se národním právem)

čl. 2 Věcná působnost

- nařízení se vztahuje na zcela nebo částečně automatizované zpracování OÚ a na neautomatizované zpracování těch OÚ, které jsou obsaženy v evidenci nebo do ní mají být zařazeny.
- nařízení se nevztahuje na zpracování OÚ při činnostech, které neupravuje právo EU (např. národní bezpečnost čl. státu EU); při výkonu činností v oblasti společné zahraniční a bezpečnostní politiky EU (Eurojust, Europol); domácí a osobní použití (výjimka – sdílení OÚ třetích osob s uživateli určité služby, např. sociální sítě); prevence, vyšetřování, odhalování či stíhání trestných činů
- nařízení se však vztahuje na instalace kamerového systému, který sleduje veřejné prostranství za účelem ochrany majetku, zdraví a života FO a její rodiny (viz rozsudek C-212/13 František Ryneš proti Úřadu pro ochranu osobních údajů)

rozsudek C-101/01 Lidquist

SDEU judikoval, že i samotné zveřejnění informací o jiné fyzické osobě na webových stránkách je zpracováním OÚ, které navíc nespadá do výjimky pro osobní a domácí činnosti. Za zpracování OÚ je proto nutné v souladu s výše uvedeným považovat jejich zveřejnění na osobních blozích či otevřených profilech na sociálních sítích.

- pokud jsou na webových stránkách např. zájmových spolků, farností apod. zveřejněny osobní údaje fyzických osob, jedná se o zpracování osobních údajů a je třeba se řídit právním předpisem upravujícím zpracování OÚ (pravděpodobně by bylo potřeba zajistit souhlas subjektu OÚ s jejich zpracováním a uvedením na webu)

čl. 3 Místní působnost

- nařízení se vztahuje na:
 - zpracování OÚ správcem či zpracovatelem z EU (bez ohledu na to, zda samotné zpracování probíhá na území EU či nikoli)
 - zpracování OÚ subjektů z EU správcem či zpracovatelem, který není z EU, ale zpracování souvisí s nabídkou služeb, zboží nebo monitorování chování na území EU
 - zpracování OÚ správcem, který není z EU, ale nařízení se na zpracování OÚ vztahuje na základě mezinárodního práva veřejného

čl. 4 Definice

- definice pojmů
 - osobní údaj
 - zpracování
 - omezení zpracování
 - profilování
 - pseudonymizace
 - evidence
 - správce
 - zpracovatel
 - souhlas

osobní údaj

- veškeré informace o identifikované nebo identifikovatelné fyzické osobě; zejména jméno, identifikační číslo, lokační údaje, síťový identifikátor, zvláštní prvky fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity
- není rozhodující, zda je údaj zcela pravdivý a objektivně měřitelný nebo zda jde o pouhý odhad charakteristiky člověka (např. odhad nákupních preferencí nebo zájmu o určitý druh literatury, informací)
- identifikovatelná osoba = osoba, kterou správce nebo zpracovatel OÚ dokáže odlišit od ostatních osob dle OÚ, které má k dispozici (i nepřímou v součinnosti s jiným subjektem)

zpracování OÚ

- jakákoliv operace nebo soubor operací s OÚ, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je: shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení, zkombinování, omezení, výmaz nebo zničení
- systematický proces za určitým účelem či cílem
- může být manuální, elektronické, s využitím software nebo kombinace
- příklad zpracování OÚ: vedení personální evidence, evidence čtenářů, databáze klientů banky
- ne každý přístup k OÚ je jejich zpracováním dle nařízení: je-li účelem zpracování OÚ práce s OÚ jako takovými, jedná se o zpracování, pokud jde o práci nahodilou a nepravidelnou, o zpracování se nejedná (např. servisní práce na hardware, software)

omezení zpracování

- označení uložených OÚ za účelem omezení jejich zpracování v budoucnu

profilování

- jakákoli forma automatizovaného zpracování OÚ směřující k hodnocení některých osobních aspektů fyzické osoby, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází nebo pohybu

pseudonymizace

- zpracování OÚ tak, že již nemohou být přiřazeny konkrétní osobě bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně opatření, která zajistí, že nebudou přiřazeny k identifikované nebo identifikovatelné fyzické osobě (např. OÚ jsou uloženy tak, že osoby, kterým OÚ patří jsou označeny čísly, jmenný seznam číslo=jméno je uložen odděleně)
- i po pseudonymizaci se jedná o OÚ dle nařízení, pseudonymizace napomáhá jejich zabezpečení
- anonymizace: anonymizované OÚ se nepovažují za OÚ a do působnosti nařízení nespádají, nelze je přiřadit ke konkrétní osobě (neexistuje jmenný seznam číslo=jméno)
- rozdíl mezi anonymizací a pseudoanonymizací je v tom, že anonymizace je nevratný proces, anonymizované údaje nelze zpětně přiřadit k fyzické osobě

evidence

- jakýkoli strukturovaný soubor OÚ přístupných podle zvláštních kritérií, ať již centralizovaný, decentralizovaný, nebo rozdělený podle funkčního či zeměpisného hlediska
- personální kartotéky, lékařské kartotéky, evidence čtenářů, evidence zákazníků, soubor jmenných autorit atd.

čl. 5 Zásady zpracování osobních údajů

- zákonnost, korektnost, transparentnost: zpracování nesmí být v rozporu se zákonem, správce OÚ musí plnit informační povinnost vůči subjektu údajů
- zásada účelového omezení: zpracování OÚ jen za účelem, kvůli kterému byly shromážděny
- zásada minimalizace údajů: zpracování OÚ nezbytně nutných pro daný účel, nelze zpracovávat OÚ jen z důvodu „jednou by se mohly hodit“
- zásada přesnosti: zpracovávat přesné OÚ
- zásada omezení uložení: zpracování OÚ jen po dobu, pokud je to nutné
- zásada integrity a důvěrnosti: povinnost zabezpečit zpracování OÚ správcem, přijetí bezpečnostních opatření
- zásada odpovědnosti: povinnost správce zajistit soulad se zásadami a být schopen soulad prokázat

čl. 6 Zákonnost zpracování

- zpracování musí být založeno na jednom z právních titulů vyjmenovaných v čl. 6:
 - souhlas se zpracováním OÚ
 - plnění smlouvy
 - splnění právní povinnosti správcem
 - ochrana životně důležitých zájmů
 - splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci
 - zpracování OÚ je nezbytné pro účely oprávněných zájmů správce OÚ

čl. 7 Podmínky vyjádření souhlasu

- správce OÚ musí být schopen doložit, že souhlas se zpracováním OÚ byl udělen (zpravidla tedy písemný souhlas)
- písemný souhlas je srozumitelný, provedený jasnými a jednoduchými jazykovými prostředky
- souhlas musí být jednoduše odvolatelný
- plnění smlouvy a následné poskytnutí služby nelze podmiňovat udělením souhlasu, pokud souhlas se zpracováním není pro tuto smlouvu a službu bezpodmínečně nutný

čl. 8 Souhlas dítěte u služeb informační společnosti

- udělení souhlasu se zpracováním OÚ dítětem
- souhlas je zákonný, pokud je dítěti nejméně 16 let. Je-li dítě mladší než 16 let musí být souhlas vyjádřen nebo schválen osobou vykonávající rodičovskou zodpovědnost vůči dítěti.
- čl. státy mohou stanovit věk nižší než 16 let, nesmí to však být méně než 13 let; Česká republika: 15 let
- správce vyvine přiměřené úsilí s ohledem na dostupnou technologii, aby ověřil, že byl souhlas vyjádřen či schválen osobou s rodičovskou zodpovědností (to může být problematické; např. uvedení emailu rodiče a následné potvrzení souhlasu dítěte rodičem)

čl. 9 Zpracování zvláštních kategorií OÚ (citlivé údaje)

- zvláštní kategorie OÚ: údaje o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, genetické údaje, biometrické údaje, údaje o zdravotním stavu, sexuálním životě, sexuální orientaci
- zpracování zvláštních OÚ je zakázáno
- výjimky ze zákazu: udělení výslovného souhlasu se zpracováním; povinnosti vyplývající z pracovního práva, sociálního zabezpečení, sociální ochrany; ochrana životně důležitých zájmů; obhajoba právních nároků a soudní pravomoc; preventivní a pracovní lékařství, posouzení pracovní schopnosti; ochrana veřejného zdraví atd.
- rodné číslo do zvláštní kategorie OÚ nepatří!

Práva subjektu údajů

- čl. 12 – 23
- transparentnost a korektnost zpracování (čl. 12 - 14)
- právo na přístup k OÚ
- právo na opravu
- právo na výmaz (právo být zapomenut)
- právo na omezení zpracování ve stanovených případech
- právo na přenositelnost údajů
- právo vznést námitku: přímý marketing, profilování, automatizované rozhodování

čl. 12 Transparentní informace, sdělení a postupy pro výkon práv subjektu údajů

- správce přijme vhodná opatření, aby poskytl subjektu údajů stručným, transparentním, srozumitelným a snadno přístupným způsobem za použití jasných a jednoduchých jazykových prostředků veškeré informace, které se týkají způsobu zpracování OÚ, které provádí
- např. srozumitelné a jasné sepsání veškerých postupů zpracování OÚ, účelu zpracování, nakládání s OÚ apod., které je snadno dostupné přes webové stránky nebo v tištěné podobě v provozovně správce

čl. 13 Informační povinnost

- při získávání OÚ od subjektu údajů správce má povinnost poskytnout tyto informace:
 - kontaktní údaje správce
 - kontaktní údaje pověřence pro ochranu OÚ
 - účel zpracování OÚ a právní základ pro zpracování
 - oprávněný zájem, pokud existuje
 - případné příjemce nebo kategorie příjemců OÚ
 - případný úmysl předat OÚ do třetí země nebo mezinárodní organizaci
 - další informace, pokud je to nezbytné: doba uložení OÚ, existence práv subjektu údajů, právo podat stížnost u ÚOOÚ atd.

čl. 13 Informační povinnost

- inf. povinnost lze řešit písemným poučením fyzické osoby o zpracování OÚ
- v praxi knihoven jsou knihovní řády doplňovány o poučení uživatele o zpracování OÚ, je dobré informovat uživatele při vyplňování přihlášky (uzavírání smlouvy o poskytnutí služeb), informace na webových stránkách

čl. 15 – 22 Práva subjektu údajů

- právo na přístup k OÚ
- právo na opravu
- právo na výmaz (právo být zapomenut)
- právo na omezení zpracování
- právo na přenositelnost údajů
- právo vznést námitku: profilování, přímý marketing, automatizované zpracování OÚ

Správce OÚ, zpracovatel, pověřenec

- čl. 24 – 43
- správce: subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování OÚ
- zpracovatel: subjekt, který zpracovává OÚ pro správce; zpracovatelem není zaměstnanec správce, ale zpravidla externí subjekt
- správce musí mít se zpracovatelem uzavřenou smlouvu o zpracování (nebo jiný obdobný dokument dle práva EU), která stanoví: předmět a dobu trvání zpracování, povahu a účel zpracování, typ osobních údajů a kategorie subjektu údajů, povinnosti a práva správce, mimo jiné je zpracovatel povinen zajistit mlčenlivost osob oprávněných zpracovávat OÚ
- záznamy o činnostech zpracování
- zabezpečení zpracování
- ohlašování případů porušení zabezpečení OÚ dozorovému úřadu

- pověřenec pro ochranu OÚ: nařízení osobu pověřence nedefinuje, vymezuje situace, kdy je správce či zpracovatel povinen pověřence jmenovat, pravomoci pověřence a úkoly, které má vykonávat
- pověřence jmenuje: orgán veřejné moci či veřejný subjekt; instituce provádějící zpracování, které vyžaduje rozsáhlé pravidelné a systematické monitorování subjektů údajů; orgány zpracovávající zvláštní kategorie OÚ nebo údajů týkajících se trestních rozsudků
- pověřenec musí mít odborné znalosti práva a praxi v oblasti ochrany OÚ
- úkoly pověřence: poskytování informací a poradenství správcům nebo zpracovatelům a zaměstnancům, monitorování souladu zpracování OÚ s nařízením, poskytování poradenství na požádání a spolupráce s dozorovým úřadem

Předávání OÚ do třetích zemí nebo mez. organizacím

- čl. 44 - 50

Nezávislé dozorové úřady

- čl. 51 – 77
- Úřad pro ochranu osobních údajů
 - dozorový úřad v ČR; je nezávislý
 - vydává metodiky, stanoviska, doporučení
 - řeší stížnosti subjektů údajů na údajné porušení ochrany OÚ, provádí kontrolní a monitorovací činnost, osvětovou činnost pro veřejnost, poradenskou činnost, vede seznam druhů operací, které podléhají požadavku na posouzení vlivu na ochranu OÚ, podporuje vypracování kodexů chování, spolupracuje s dalšími dozorovými úřady a Evropským sborem pro ochranu osobních údajů
 - oprávněn ukládat správní pokuty v souvislosti s porušením nařízení

- Evropský sbor pro ochranu osobních údajů
 - původně jako pracovní skupina 29 (WP29) ustanovená dřívější směrnicí
 - zajišťuje jednotné uplatňování nařízení, má rozsáhlé pravomoci, vydává pokyny a stanoviska k postupům a činnostem dozorových úřadů čl. států EU, ke kodexům chování, podporuje spolupráci dozorových úřadů, konzultační činnost, poskytuje poradenství ve věcech ochrany a zpracování OÚ Evropské komisi

Právní ochrana a sankce

- čl. 77 – 84
- právo podat stížnost u dozorového úřadu: podává subjekt údajů, pokud se domnívá, že zpracováním jeho osobních údajů je porušeno toto nařízení
- právo na účinnou soudní ochranu vůči dozorovému úřadu: soudní ochrana proti závaznému rozhodnutí dozorového úřadu, nejprve je třeba vyčerpat řádné opravné prostředky v řízení před správním orgánem (rozklad); soudní ochrana před nečinností úřadu při řešení stížnosti
- soudní ochrana vůči správci nebo zpracovateli
- právo na náhradu újmy
- správní pokuty
- jiné sankce za porušení, na která se nevztahují správní pokuty

Zvláštní situace zpracování OÚ

- čl. 85 – 91
- čl. státy uvedou prostřednictvím právních předpisů právo na ochranu osobních údajů podle nařízení do souladu s právem na svobodu projevu a informací, včetně zpracování pro novinářské účely a pro účely akademického, uměleckého či literárního projevu
- OÚ v úředních dokumentech, které jsou v držení orgánu veřejné moci či veřejného nebo soukromého subjektu za účelem plnění úkolu ve veřejném zájmu, může tento orgán či subjekt zpřístupnit v souladu s právem EU nebo čl. státu, tak aby zajistil soulad mezi přístupem veřejnosti k úř. dokumentům a právem na ochranu OÚ podle nařízení

- zpracování národních identifikačních čísel
- čl. státy mohou dále stanovit zvláštní podmínky pro zpracování národních identifikačních čísel nebo jakýchkoliv jiných všeobecně uplatňovaných identifikátorů. V takovém případě se národní identifikační číslo použije pouze v závislosti na vhodných zárukách práv a svobod daného subjektu údajů podle tohoto nařízení
- v ČR rodná čísla upravená v § 13 zákona o evidenci obyvatel; není citlivým údajem

Prováděcí akty, závěrečná ustanovení

- čl. 94 – 99
- čl. 96 vztah k dříve uzavřeným dohodám: mezinárodní dohody, které byly uzavřeny před datem 24. 5. 2016 (nařízení vstoupilo v platnost 25. 5. 2016) a jsou v souladu s právem EU, zůstávají v platnosti, dokud nebudou změněny, nahrazeny či zrušeny.
- čl. 94: zrušení směrnice 95/46/ES, která upravovala zpracování OÚ dříve; stávající odkazy na tuto směrnici jsou považovány za odkazy na nařízení
- legisvakanní doba: 25. 5. 2016 – 24. 5. 2018

Zákon o zpracování osobních údajů

zákon č. 110/2019 Sb., zákon o ochraně osobních údajů a o změně některých zákonů

- upravuje: zpracování OÚ podle nařízení GDPR, zpracování OÚ související s trestnou činností a jejím postihováním, s bezpečností ČR, se zajišťování veřejného pořádku, se zajišťováním obranných a bezpečnostních zájmů ČR a další zpracování OÚ
- správce je oprávněn zpracovávat OÚ, pokud je to nezbytné pro plnění povinností uložených právním předpisem nebo pro naplnění veřejného zájmu a při výkonu veřejné moci – *výslovné uvedení, aby nedocházelo k pochybnostem, pokud by toto oprávnění nebylo výslovně uvedeno v jiných předpisech správního práva*

Zákon o zpracování osobních údajů

- výjimka z posuzování slučitelnosti účelů zpracování OÚ: povinnost posuzovat slučitelnost vyplývá z nařízení GDPR; při zajišťování chráněného zájmu není nutné slučitelnost posuzovat, chráněný zájem = obranný nebo bezpečnostní zájem ČR, veřejný pořádek, vnitřní bezpečnost, odhalování trestné činnosti, ochrana nezávislosti soudů a soudců, ochrana práv a svobod osob atd.; další výjimky na základě chráněných zájmů – *účelem je usnadnit zpracování OÚ v souvislosti s chráněným zájmem*
- výjimka z povinnosti posouzení vlivu zpracování OÚ na ochranu OÚ: není třeba posuzovat vliv, pokud správce má zákonnou povinnost takové zpracování OÚ provádět

Zákon o zpracování osobních údajů

- zpracování OÚ za účelem vědeckého nebo historického výzkumu nebo pro statické účely: povinnost zajistit dodržování konkrétních opatření pro ochranu zájmů subjektu osobních údajů
- zpracování OÚ prováděné pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu: není podmíněno schválením Úřadu pro ochranu osobních údajů a náleží mu ochrana zdroje a obsahu informací
- ochrana zdroje a obsahu informací, výjimky týkající se novinářského účelů zpracování OÚ a akademického, uměleckého nebo literárního projevu

Zákon o zpracování osobních údajů

- organizace a činnost Úřadu pro ochranu osobních údajů:
 - sídlí v Praze
 - je nezávislý
 - upozorňuje správce nebo zpracovatele na hrozící porušení povinností při jejich způsobu zpracování OÚ
 - stanoví vyhláškou kritéria pro vydávání osvědčení o zpracování OÚ a pro monitorování kodexů chování při zpracování OÚ
 - schvaluje kodexy chování
 - zpracovává výroční zprávy o své činnosti
 - zajišťuje plnění povinností vyplývajících z mezinár. smluv a z předpisů EU
 - řeší stížnosti a přestupky v oblasti zpracování OÚ, vybírá pokuty

Zákon o zpracování osobních údajů

- přestupky a sankce:

- fyzická osoba, právnická osoba nebo fyzická osoba-podnikatel se dopustí přestupku, když poruší zákaz zveřejnění OÚ stanovený trestním řádem nebo zákonem o soudnictví ve věcech mládeže – sankce 1 mil. Kč nebo 5 mil. Kč, pokud je přestupek spáchán např. pomocí tisku, filmu, rozhlasu, televize...

Zákon o zpracování osobních údajů

- přestupky a sankce:
 - správce nebo zpracovatel se dopustí přestupku např. tím, že poruší některou ze základních zásad pro zpracování OÚ, poruší některé z práv subjektu údajů, neposkytne Úřadu pro ochranu osobních údajů přístup k údajům, informacím a prostorám
 - dle charakteru přestupku lze uložit pokutu ve výši až 10 000 000 EUR nebo 2% celkového ročního obrátu celosvětově, pokud jde o podnik, nebo ve výši až 20 000 000 EUR nebo 4% celkového ročního obrátu celosvětově, pokud jde o podnik
 - velké množství dalších přestupků při zpracování OÚ

Použitá literatura

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) – **obecné nařízení GDPR**

NULÍČEK, Michal. *GDPR - obecné nařízení o ochraně osobních údajů*. 2. vydání. Praha: Wolters Kluwer, 2018. Praktický komentář. ISBN 978-80-7598-068-7.

Zákon č. 110/2019 Sb., o zpracování osobních údajů