

Obecné nařízení o ochraně osobních údajů (GDPR)

Základní informace k Obecnému nařízení o ochraně osobních údajů (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 \(Obecné nařízení o ochraně osobních údajů\)](#), v anglickém jazyce General Data Protection Regulation – GDPR (dále jen „Obecné nařízení“) bylo přijato v dubnu 2016, ale účinnosti nabude až 25. května 2018. V České republice tak nahradí současnou právní úpravu ochrany osobních údajů v podobě směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a související zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Obecné nařízení představuje nový právní rámec ochrany osobních údajů v evropském prostoru, který hájí práva občanů proti neoprávněnému zacházení s jejich daty a osobními údaji. Obecným nařízením se bude především, pokud jde o povinnosti, řídit subjekt, který pracuje s osobními údaji. Takový subjekt je nazýván správcem osobních údajů. Obecným nařízením se řídí i zpracovatel osobních údajů, což je subjekt, který pro správce osobních údajů osobní údaje zpracovává. Pokud jde o práva vyplývající z Obecného nařízení, ta vyplývají fyzické osobě, což je subjekt údajů. Dále se Obecným nařízením budou řídit i dozorové úřady, tj. i Úřad pro ochranu osobních údajů, který bude uplatňovat svěřené pravomoci za účelem plnění stanovených úkolů.

Obecné nařízení s sebou přinese rovnocennou vymahatelnost práva v celé EU, stejné sankce a mnohem těsnější spolupráci dozorových orgánů. Dopadne totiž skutečně na každého, kdo s osobními údaji při svém podnikání či působení pracuje.

Úřad pro ochranu osobních údajů vydal [soubor otázek a odpovědí](#), které se vztahují k problematice Obecného nařízení, a na základě svých zkušeností vytvořil přehled [deseti největších omylů o obecném nařízení](#). Reaguje tak na nepřesnosti či zavádějící informace týkající se Obecného nařízení.

Důvody pro přijetí Obecného nařízení o ochraně osobních údajů (GDPR)

Ustanovení bodu 9 preambule Obecného nařízení konstatuje, že základní cíle a zásady stávající zrušované směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů, tedy zajišťovat ochranu základních práv a svobod fyzických osob, zejména jejich soukromí v souvislosti se zpracováním osobních údajů, i nadále platí. Zároveň je ale poukazováno na dosavadní roztříštěnost při provádění ochrany osobních údajů v rámci států EU. Proto je nezbytné dosáhnout nového soudržnějšího rámce vymahatelných pravidel, který by, ačkoli se zdůrazňuje technologická neutralita, měl umožnit rozvoj digitální ekonomiky na celém vnitřním trhu, resp. účinně reflektovat technologický rozvoj a globalizaci.

Zásady zpracování osobních údajů dle Obecného nařízení o ochraně osobních údajů (GDPR)

- Zákonnost, korektnost, transparentnost – správce osobních údajů musí zpracovávat osobní údaje na základě nejméně jednoho právního důvodu a vůči subjektu údajů transparentně,
- omezení účelu - osobní údaje musí být shromažďovány pro určité a legitimní účely a nesmějí být zpracovávány neslučitelným způsobem s těmito účely,
- minimalizace údajů - osobní údaje musí být přiměřené a relevantní ve vztahu k účelu, pro který jsou zpracovávány,
- přesnost - osobní údaje musí být přesné,
- omezení uložení - osobní údaje by měly být uloženy ve formě umožňující identifikaci subjektu údajů jen po nezbytnou dobu pro dané účely, pro které jsou zpracovávány,
- integrita a důvěrnost - technické a organizační zabezpečení osobních údajů.

Jednotlivé zásady jsou rozvinuty v článku 5 odst. 1 Obecného nařízení. Vymezení, resp. dodržování těchto zásad, je pro správce osobních údajů zásadní, nejen z toho důvodu, že to jsou de facto zároveň povinnosti, ale i proto, že v článku 5 odst. 2 Obecného nařízení je stanovena odpovědnost správce osobních údajů za jejich dodržování a zároveň povinnost správce osobních údajů být schopen dodržování těchto zásad (povinností) doložit. Jde o vyjádření tzv. principu odpovědnosti správce osobních údajů. K prokazování souladu s těmito zásadami budou sloužit záznamy o činnostech zpracování a též kodexy a osvědčení.

Základní povinnosti, které přináší Obecné nařízení o ochraně osobních údajů (GDPR)

- Povinnost vést záznamy o činnostech zpracování,
- posouzení vlivu na ochranu osobních údajů,
- předchozí konzultace s Úřadem pro ochranu osobních údajů,
- ohlašování případu porušení zabezpečení osobních údajů Úřadu pro ochranu osobních údajů,
- oznamování případu porušení zabezpečení osobních údajů subjektu údajů,
- povinnost jmenovat **pověřence pro ochranu osobních údajů** nebo takovou osobu zajistit externě.

Institut pověřence pro ochranu osobních údajů dle Obecného nařízení o ochraně osobních údajů (GDPR)

Ode dne 25. května 2018, kdy se Obecné nařízení stane bezprostředně účinné a aplikovatelné ve všech členských státech EU, jsou mimo jiné všechny obce povinny mít tzv. **pověřence pro ochranu osobních údajů** a plnit další povinnosti s tím související. **Každou obec je totiž nutné chápat jako orgán veřejné moci** ve smyslu článku 37 Obecného nařízení, jemuž Obecné nařízení povinnost zřídit funkci pověřence pro ochranu osobních údajů ukládá. Orgánem veřejné moci jsou v podmínkách obcí nepochybně též školy ve formě školské právnické osoby či příspěvkové organizace, neboť i ty jsou nadány pravomocí rozhodovat o právech a povinnostech fyzických osob. Povinnost mít pověřence pro ochranu osobních údajů Obecné nařízení dále vztahuje i na ty instituce nebo subjekty, jejichž hlavní činnost a) vyžaduje pravidelné a systematické monitorování subjektů údajů ve velkém měřítku (např. provozovatelé městské hromadné dopravy, kteří provádí evidenci cestujících) nebo b) spočívá

v rozsáhlém zpracování citlivých údajů (např. nemocnice nebo sociální zařízení). Všechny tyto subjekty tedy budou muset mít s účinností od 25. května 2018 pověření pro ochranu osobních údajů.

Hlavní úkoly pověření pro ochranu osobních údajů jsou uvedeny v článku 39 Obecného nařízení.

Prvním úkolem pověření pro ochranu osobních údajů je *„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“*. Toto ustanovení ukládá pověřenci pro ochranu osobních údajů seznámit správce osobních údajů a zpracovatele osobních údajů s povinnostmi vyplývajícími z ochrany osobních údajů a zajistit dostatečné porozumění těmto povinnostem.

Druhým úkolem pověření pro ochranu osobních údajů je *„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“*.

Třetím úkolem pověření pro ochranu osobních údajů je *„poskytování poradenství na požádání, pokud jde o posouzení vlivu na ochranu osobních údajů, a monitorování jeho uplatnění podle článku 35“*. Pověřenec pro ochranu osobních údajů by měl dohlížet nebo spolupracovat na posouzení vlivu na ochranu osobních údajů.

Čtvrtý úkol pověření pro ochranu osobních údajů souvisí s dohledem kontrolního orgánu. Povinností pověření pro ochranu osobních údajů je: *„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“*. V případě České republiky je dozorovým orgánem Úřad pro ochranu osobních údajů. Pověřenec pro ochranu osobních údajů tak zajišťuje přímý a bezprostřední kontakt s kontrolním orgánem, tedy Úřadem pro ochranu osobních údajů. Komunikační povinnost pověření pro ochranu osobních údajů však není jen ve vztahu ke kontrolnímu orgánu, ale také směrem k subjektům údajů, tedy lidem. K povinnostem organizací patří zveřejnit kontakt na pověření pro ochranu osobních údajů tak, aby tento kontakt byl veřejně přístupný a snadno dohledatelný.

Ministerstvo vnitra k problematice pověření pro ochranu osobních údajů vypracovalo [metodické doporučení k činnosti obcí k organizačně – technickému zabezpečení funkce pověření pro ochranu osobních údajů podle obecného nařízení o ochraně osobních údajů v podmínkách obcí](#). Toto metodické doporučení je zaměřeno na výklad k institutu pověření pro ochranu osobních údajů za účelem zodpovězení praktických otázek a poskytnutí návodu, jak **organizačně zabezpečit plnění povinností souvisejících s ustanovením pověření pro ochranu osobních údajů v podmínkách obcí**.

Návrh nového zákona o zpracování osobních údajů

Ministerstvo vnitra předložilo podle Plánu legislativních prací vlády na rok 2017 [návrh zákona o zpracování osobních údajů](#). Návrh zákona o zpracování osobních údajů má nahradit stávající zákon č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů. Novelizace zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů se vzhledem k nutnosti implementovat sekundární právní předpisy EU a vzhledem k nutnému rozsahu změn ukázala jako velice nepraktická. Návrh zákona o zpracování osobních údajů reaguje na přijetí Obecného nařízení a adaptuje právní řád na požadavky Obecného nařízení, včetně povolených výjimek a odchylek nebo úpravy vztahu mezi ochranou osobních údajů a svobodou projevu. Návrh zákona o zpracování osobních údajů rovněž zachovává ustanovení, která se vztahují k působení Úřadu pro ochranu osobních údajů, přičemž se částečně mění jeho struktura. Návrh zákona o zpracování osobních údajů již nadále nepočítá s funkcí inspektorů, nově budou strukturu Úřadu pro ochranu osobních údajů tvořit pouze předseda a 2 místopředsedové. Tato změna povede k tomu, aby Úřad pro ochranu osobních údajů byl schopen plnit svoje povinnosti stanovené v Obecném nařízení.

Obecné nařízení zavádí celou řadu nových pravidel. Jejich aplikaci a dodržování bude muset každý správce osobních údajů i zpracovatel osobních údajů prokazatelně doložit po celou dobu zpracování.

Metodická pomoc v oblasti ochrany osobních údajů

Obecně je k výkonu dozoru a kontroly nad samostatnou působností svěřenou obcím příslušné [Ministerstvo vnitra](#), přičemž mezi základní principy výkonu dozoru a kontroly patří zejména předcházení vzniku nedostatků a důraz je v této souvislosti kladen na poskytování metodické pomoci obcím. V případě ochrany osobních údajů se jedná o samostatnou působnost obcí, k poskytování metodické pomoci obcím tedy bude příslušné Ministerstvo vnitra.

Ministerstvo vnitra připravilo [nové internetové stránky](#) k problematice ochrany osobních údajů. Na webových stránkách naleznete [právní předpisy](#), [metodická doporučení](#), [odpovědi na nejčastější otázky](#) stejně jako odkazy na [další relevantní informace](#) a zainteresované instituce. Zveřejněn je i odkaz na Ministerstvem vnitra iniciovaného robota na chatování k GDPR (tzv. [Chatbot GDPR](#)), kterému je možné klást základní dotazy a získat tak primární přehled o této problematice. Ministerstvo vnitra také připravilo pro obce pomůcku pro rychlou kontrolu organizačního zabezpečení ochrany osobních údajů podle obecného nařízení – tzv. kontrolní seznamy ([checklisty](#)) pro obce.

Metodickou pomoc poskytují i jiné orgány veřejné správy v rámci své působnosti, např. Ministerstvo zdravotnictví vydalo [metodickou pomůcku k aplikaci GDPR ve zdravotnictví](#) a Ministerstvo školství vydalo [metodickou pomůcku k aplikaci GDPR ve školství](#).

Dle zákona č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve znění pozdějších předpisů [Úřad pro ochranu osobních údajů](#) provádí dozor nad dodržováním povinností stanovených zákonem č. 101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů, ve

znění pozdějších předpisů při zpracování osobních údajů a poskytuje konzultace a osvětu v oblasti ochrany osobních údajů. Je tedy dozorovým orgánem v oblasti ochrany osobních údajů a poskytuje metodickou pomoc týkající se ochrany osobních údajů.

Kontakty pro dotazy a konzultace

Úřad pro ochranu osobních údajů

kontaktní adresa: posta@uouu.cz

Odbor bezpečnostní politiky a prevence kriminality Ministerstva vnitra pro otázky týkající se Obecného nařízení

kontaktní adresa: obppk@mvcz.cz

Odbor legislativy a koordinace předpisů Ministerstva vnitra pro otázky týkající se zákona č. 312/2002 Sb., o úřednících územních samosprávných celků a o změně některých zákonů

kontaktní adresa: ol@mvcz.cz

Odbor veřejné správy, dozoru a kontroly Ministerstva vnitra pro otázky týkající se zákona č. 128/2000 Sb., o obcích (obecní zřízení)

kontaktní adresa: odbordk@mvcz.cz

Užitečné odkazy

GDPR a role ÚOOÚ <https://www.uouu.cz/gdpr-a-role-uouu/ds-4726/archiv=0&p1=3938>

Dokumenty k GDPR <https://www.uouu.cz/dokumenty-k-gdpr/ds-4720/archiv=0&p1=3938>

Základní příručka k GDPR <https://www.uouu.cz/zakladni-prirucka-k-gdpr/ds-4744/p1=4744>

<https://www.gdpr.cz/>

<http://www.eugdpr.org/> (v angličtině)

Vypracovala: Mgr. Klára Škrlová