

Obsah

Obecné nařízení GDPR

Kořenského 15/1107, 150 00 Praha 5

+420 257 312 083

advokátní kancelář



■ RYCHETSKÝ ■ HLAVÁČEK ■ KRAMPERA ■

akrhk@akrhk.cz

Obec jako správce osobních údajů

Obce spravují a zpracovávají osobní údaje na základě nejrůznějších zákonů:

- zákon č. 128/2000 Sb., o obcích
- zákon č. 491/2001 Sb., o volbách do zastupitelstev obcí,
- zákon č. 565/1990 Sb., o místních poplatcích.

Jako správci osobních údajů mohou jejich zpracováním pověřit jiné (společnost spravující obecní bytový fond).

Jsou zpracovateli osobních údajů pro jiné – typicky pro Ministerstvo vnitra (evidence obyvatel) nebo pro Ministerstvo dopravy (agenda ŘP).



Změny v GDPR

- Zpřísňují se parametry, požadované pro **platné** udělení souhlasu se zveřejněním osobních údajů dotčenou osobou (svobodný, konkrétní, informovaný a jednoznačný projev vůle),
- Prohlubují se požadavky na **informovanost** dotčených osob o zpracování jejich osobních údajů
- Rozšiřují se **práva dotčených osob vůči správcům** jejich osobních údajů.
- Upřesňují se povinnosti správce osobních údajů, pokud jde o **organizační zajištění** plnění jejich povinností
- Zvyšují se nároky na **bezpečnost** zpracování osobních údajů ze strany zpracovatelů
- Sjednocuje se **výkon dozoru** nad správci a zpracovateli

Zákonnost zpracování dle GDPR (čl. 6)

Zpracování je zákonné, pouze pokud je splněna nejméně jedna z těchto podmínek a pouze v odpovídajícím rozsahu:

- subjekt údajů **udělil souhlas** se zpracováním svých osobních údajů pro jeden či více konkrétních účelů;
- zpracování je nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů;
- zpracování je nezbytné pro splnění právní povinnosti, která se na správce vztahuje
- zpracování je nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
- zpracování je **nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci**, kterým je pověřen správce
- zpracování je nezbytné pro účely oprávněných zájmů příslušného 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 (první pododstavec se netýká zpracování prováděného orgány veřejné moci při plnění jejich úkolů).

Chystaný zákon o zpracování osobních údajů (stav v září 2017)

§ 13 „Orgány veřejné moci a veřejné subjekty“ podle překladu čl. 37 odst. 1 písm. a) Obecného nařízení o ochraně osobních údajů (anglicky *a public authority or body*, francouzsky *une autorité publique ou un organisme public*, německy *Behörde oder öffentlichen Stelle*) lze chápat velmi široce podle logiky předpisů o přístupu k informacím jako:

- Ministerstva, další ústřední orgány státní správy, další jim podřízené úřady (cca 50)
- **Obce všech kategorií (cca 6 250)** a kraje (14)
- Všechny soudy (97)
- Všechny příspěvkové organizace (přes 10 000)
- Státní podniky (20) a případně další veřejné ústavy atd.
- Veřejné školy (asi 10 000)
- Veřejné nebo ozbrojené sbory (Policie, HZS, Armáda ...)
- Komory (ČAK, ČLK, ...).

Smyslem článku 37(1)(a) není kontrola moci ze strany veřejnosti, ani kontrola hospodaření s veřejnými prostředky, jako u zákona 106/1999 Sb. a dalších předpisů o přístupu k informacím. **Pokud například obec založí s.r.o. na opravu silnic, nemá zřízení pověřence pro ochranu dat v takové s.r.o. žádnou přidanou hodnotu a představuje administrativní zátěž a náklad navíc.**

Chystaný zákon o zpracování osobních údajů (stav v září 2017)

§ 14

- Obecné nařízení o ochraně osobních údajů v článku 43(1) vyžaduje, aby členské státy určily, zda bude subjekty, které budou certifikovat (osvědčovat) splnění požadavků různých dobrovolných pečetí, známek nebo certifikátů ochrany soukromí, akreditovat dozorový úřad (v ČR tedy ÚOOÚ), nebo **akreditační orgán** určený v souladu s nařízením č. 765/2008(ES), kterým je v ČR podle § 15 odst. 1 a 4 zákona č. 22/1997 Sb., o technických požadavcích na výrobky, ve znění pozdějších předpisů, a navazujícího sdělení Ministerstva průmyslu a obchodu vyhlášeného pod č. 385/2010 Sb. ustanoven Český institut pro akreditaci, o.p.s.
- Na základě jednání mezi oběma institucemi se zvolila varianta druhá.

Změny souvisejících zákonů (stav k září 2017)

- Zákon o civilním letectví
- Zákon o Policii České republiky, Zákon o Generální inspekci bezpečnostních sborů, Zákon o Vojenské policii
- Zákon o státním zastupitelství
- Zákon o Probační a mediační službě, Zákon o Rejstříku trestů
- Zákon o Vězeňské službě a justiční stráží České republiky
- Zákon o soudech a soudcích, Zákon o Ústavním soudu
- Trestní řád, Občanský soudní řád, Soudní řád správní, Zákon o mezinárodní justiční spolupráci
- Daňový řád
- Zákon o Finanční správě, Zákon o Celní správě, Zákon o státní službě
- Zákon o svobodném přístupu k informacím

Změna v daňovém řádu

§ 59a **Zpracování údajů správcem daně**

(1) Správce daně při zpracování osobních údajů

- a) nemusí poskytovat osobě, které se tyto údaje týkají (dále jen „subjekt údajů“), informace o tom, že dochází ke zpracování osobních údajů vztahujících se k této osobě,
- b) nemusí omezit zpracování osobních údajů v případě, že subjekt údajů popírá jejich správnost nebo vznesl námitku proti tomuto zpracování,
- c) může provádět výkon správy daní výhradně na základě automatizovaného zpracování osobních údajů.

(2) Právo vznést námitku nebo jiný prostředek ochrany proti zpracování osobních údajů uplatňuje subjekt údajů prostřednictvím stížnosti.

Pracovní skupina dle článku 29 (WP-29) k přenositelnosti údajů

- Přenositelnost údajů je v první řadě **právo subjektu údajů získat určitý podsoubor osobních údajů**, jež se ho týkají, zpracovaných správcem a uchovávat je pro další osobní použití.
- V tomto ohledu přenositelnost údajů doplňuje právo na přístup. Údaje mají být ve „*ve strukturovaném, běžně používaném a strojově čitelném formátu*“.
- Například může mít subjekt údajů zájem získat svůj aktuální playlist (historii poslouchaných skladeb) z hudebního přenosu přes internet, aby zjistil, kolikrát si pustil určitou skladbu nebo se podíval, jakou hudbu si chce koupit nebo poslouchat na jiné platformě.
- Může také chtít získat přehled kontaktů ze své webmailové aplikace, například kvůli sestavení seznamu svatebních hostů.
- Nebo může jít o získání informace o nákupech přes různé věrnostní karty, či posouzení své uhlíkové stopy.

Přenositelnost údajů se nevztahuje na případy zpracování při výkonu veřejné moci

- Obecné nařízení neustanovuje obecné právo na přenositelnost pro případy, kde zpracování osobních údajů není založeno na souhlasu nebo smlouvě.
- Přenositelnost údajů se nevztahuje na případy, kdy zpracování údajů je nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je správce pověřen nebo pokud správce plní veřejné nebo právně stanovené povinnosti.
- Není to však vyloučeno: Příkladem může být **státní služba umožňující snadné stažení dříve podaných daňových přiznání.**

Pracovní skupina dle čl. 29 (WP-29) k pověřencům

- Někteří správci a zpracovatelé musí podle Obecného nařízení povinně jmenovat pověřence. Je to **povinnost všech orgánů veřejné moci a veřejných subjektů** (bez ohledu na to, jaká data zpracovávají).
- Pověřenec musí být **dosažitelný**. Musí být schopen účinně komunikovat se subjekty údajů a spolupracovat s příslušným dozorovým úřadem.
- Dosažitelnost pověřence lze zajistit různě: fyzicky na stejném pracovišti jako zaměstnanci, přes horkou linku nebo bezpečné komunikační prostředky.

Požadavky na pověřence

- **Přiměřená úroveň odborných znalostí**
- **Profesní kvality:** podstatné musí být vědomosti z oblasti národní a evropské legislativy a praxe v oboru ochrany osobních údajů a důkladná znalost Obecného nařízení. Prospěšné by bylo, kdyby dozorové úřady propagovaly náležité a pravidelné školení pověřenců.
- **Schopnost plnit úkoly:** Osobní kvality by měly zahrnovat například integritu a vysokou úroveň profesionální etiky.
- Správce nebo zpracovatel: musí **zveřejnit kontaktní údaje pověřence** a sdělit kontaktní údaje pověřence příslušnému dozorovému úřadu

Postavení a nezávislost pověřence

Organizace by měla zajistit, aby:

- pověřenec byl pravidelně zván na schůze vyššího a středního managementu.
- byl přítomen tam, kde se dělají rozhodnutí s dopadem do ochrany osobních údajů.
- Pro případ nesouhlasu s jeho doporučením doporučuje WP29 zadokumentovat důvody, proč pověřencova rada nebyla následována.

Nesmí dostávat pokyny, jakého výsledku se má dosáhnout, jak prošetřovat stížnost nebo zda konzultovat dozorový úřad.

Nesmí být správcem nebo zpracovatelem propuštěn ani sankcionován v souvislosti s plněním svých úkolů.

Nesmí být ve střetu zájmů: typicky by neměl zastávat funkci ve vyšším managementu.

Doporučení 1: Souhlasy

Katalogizovat veškeré agendy, při kterých dochází ke zpracování osobních údajů, a rozdělil je do skupin agend, v nichž

- obec vystupuje jako zpracovatel pro jiné správce
- obec je sama správcem údajů, přičemž jde o případy, kdy
 - spravované údaje obec zpracovává vlastními organizačními útvary, a
 - zadává zpracování údajů jiným zpracovatelům.

Revidovat veškeré dosud přijaté souhlasy a ověřit, zda dostatečně splňují nově vyžadované parametry.

Pro jednotlivé skupiny agend stanovit postup, jakým bude vyžadován souhlas od dotčených osob, ať už se bude jednat o souhlasy nové, nebo o souhlasy aktualizované. Konkrétně:

- Nastavit kontrolní mechanismy k ověření, zda správci, pro které obec osobní údaje zpracovává, vydali k tomu včas potřebné a dostatečné pokyny
- Pro každou agendu vypracovat samostatné písemné znění souhlasu, na kterém dotčené osoby budou prokazatelně projevovat vůli souhlas udělit
 - Pro konkrétní agendu, při které ke zpracování údajů dochází, přičemž v agendách, kdy pro obec zpracovávají osobní údaje jiní zpracovatelé, bude zároveň existovat závazný pokyn nebo závazkový vztah, ukládající těmto zpracovatelům povinnost zajistit od dotčených osob jejich souhlasy v požadované formě (i zpětně).

Doporučení 2: Výmazy

- Stanovit technické a procesní postupy pro nárokový výmaz osobních údajů.
- V rámci katalogizace agend dle předchozího Doporučení 1. určit, kde souhlasy nesplňují parametry požadované GDPR, a zajistit stanoveným postupem jejich výmaz v případě, že se ke dni účinnosti GDPR nepodaří neplatný souhlas nahradit souhlasem platným.
- Stanovit organizační postupy pro **pravidelné prověřování**, zda shromážděné a zpracované údaje nejsou z hlediska účelu neaktuální, a **procesní postupy pro vymazání takových údajů**.
- Stanovit procesní postupy pro podání a vyřízení úkonů dotčených osob, které mají v úmyslu odvolat svůj souhlas nebo vznést námitky proti zpracování svých osobních údajů.
- O stanovení postupů dle tohoto doporučení informovat dotčené osoby v textu písemného souhlasu, připraveného dle předchozího Doporučení 1.

Doporučení 3: Přenositelnost

- V rámci katalogizace agend dle předchozího Doporučení 1 vytipovat agendy, při nichž dochází k automatizovanému shromažďování a zpracování takových osobních údajů se souhlasem dotčených osob.
- Ověřit, zda a které z nich jsou zpracovávány nezbytně pro plnění úkolů prováděných ve veřejném zájmu a zda jsou dostupné v běžném, strukturovaném a strojově čitelném formátu, umožňujícím přenositelnost, případně zajistit, aby takto dostupné byly
- Pro jednotlivé agendy posoudit, zda a za jakých okolností by se jejich přenos mohl dotknout práv osob třetích, a připravit procesní postup, jak požadavek na zajištění přenosu takových údajů odmítnout.

Doporučení 4: Pověřenec

- Rozhodnout, zda obec bude funkci pověřence **zajišťovat vlastním pracovníkem, nebo zda ji bude outsourceovat.**
- Vyčlenit pro to potřebné prostředky
- V přiměřeném předstihu prozkoumat vlastní personální rezervy, nabídku na pracovním trhu / trhu služeb a stanovit postup fyzického zajištění osoby pověřence ke dni účinnosti GDPR.

Doporučení 5: Ohlašování Úřadu

- Ověřit, zda personální a technické vybavení zadavatele odpovídá požadavkům GDPR pro zabezpečení údajů (čl. 32 – pravidelné testování účinnosti a odolnosti) a pro plnění ohlašovací povinnosti (čl. 33)

Článek 33: Ohlašování případů porušení zabezpečení osobních údajů úřadu

- 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. Pokud není ohlášení dozorovému úřadu učiněno do 72 hodin, musí být současně s ním uvedeny důvody tohoto zpoždění.
- Ohlašuje se: **co se stalo a kolik může být dotčených subjektů, jaké mohou mít následky, jaká opatření byla přijata, kdo je pověřencem**

Doporučení 6: Standardy

- Monitorovat metodickou činnost Úřadu na ochranu osobních údajů a Ministerstva vnitra směřující k definování parametrů kodexů chování tak, aby se mohly stát součástí zabezpečovací strategie veřejnoprávních správců a zpracovatelů osobních údajů.
- Monitorovat trh služeb a informační kampaně Úřadu na ochranu osobních údajů s cílem podchytit nabídky na certifikaci operací veřejných správců a zpracovatelů při nakládání s osobními údaji a rozhodnout, zda bude vhodné certifikaci podstoupit.

Doporučení 7 (pro jistotu)

- Prověřit, zda některý z existujících zpracovatelů osobních údajů, spravovaných městem, nemá sídlo mimo území ČR.

Děkuji za pozornost

Kořenského 15/1107, 150 00 Praha 5

+420 257 312 083

advokátní kancelář



■ RYCHETSKÝ ■ HLAVÁČEK ■ KRAMPERA ■

akrhk@akrhk.cz