1. **Veřejnoprávní ochrana autorského práva**

(verejnopravna ochrana dusevneho vlastnictva)

**OBECNE: Odpovědnost za porušení autorského práva**

Kdo neoprávněně, tedy bez souhlasu nositele autorského práva a práv souvisejících s právem autorským, nakládá s dílem, uměleckým výkonem, zvukově či obrazově - zvukovým záznamem nebo vysíláním rozhlasu nebo televize, které jsou předmětem ochrany podle autorského zákona, dopouští se porušení autorského práva a práv s ním souvisejících a měl by si být vědom nepříznivých důsledků, které pro něho z jeho jednání vyplývají.

**Odlišujeme tři základní typy odpovědnosti** (které mohou v důsledku porušování autorského práva vyvstat):

1. občanskoprávní
2. přestupkovou
3. trestní odpovědnost

[**OBČANSKOPRÁVNÍ ODPOVĚDNOST:**](http://www.cpufilm.cz/new/www/obcanskopravniodpovednost.html) Autorský zákon ve svém § 40 vymezuje nároky, kterých se může autor domáhat v občanskoprávním řízení v případě, že bylo do jeho práva neoprávněně zasaženo, nebo pokud jeho právu hrozí neoprávněný zásah. Autor se může domáhat:

* určení svého autorství,
* zákazu ohrožení svého práva, včetně hrozícího opakování,
* nebo neoprávněného zásahu do svého práva,
* sdělení údajů o způsobu a rozsahu neoprávněného užití,
* odstranění následků zásahu do práva, zejména stažením či zničením neoprávněně zhotovené rozmnoženiny či napodobeniny,
* poskytnutí přiměřeného zadostiučinění za způsobenou nemajetkovou újmu, zejména omluvou či zadostiučiněním v penězích a zákazu poskytování služby, kterou využívají třetí osoby k porušování nebo ohrožování práva autora.

Zákon dále v § 40 odst. 4 stanoví, že právo na náhradu škody a na vydání bezdůvodného obohacení podle zvláštních právních předpisů tedy občanského zákoníku zůstává nedotčeno a, že místo skutečně ušlého zisku se autor může domáhat náhrady ušlého zisku ve výši odměny, která by byla obvyklá za získání takové licence v době neoprávněného nakládání s dílem. Výše bezdůvodného obohacení vzniklého na straně toho, kdo neoprávněně nakládal s dílem, aniž by k tomu získal potřebnou licenci, pak činí dvojnásobek odměny, která by byla za získání takové licence obvyklá v době neoprávněného nakládání s dílem.

[**PŘESTUPKOVÁ ODPOVĚDNOST:**](http://www.cpufilm.cz/new/www/prestupkovaodpovednost.html) V méně závažných případech, kdy neoprávněné jednání nenaplňuje znaky trestného činu porušení autorského práva, práv souvisejících s právem s práv k databázi podle § 270 trestního zákoníku, a je tak klasifikováno jako přestupek, hrozí porušiteli na základě §105a – 105c autorského zákona pokuta až 150 000,- Kč. Vyšetřující policejní orgán ve spolupráci se státním zástupcem posoudí:

* intenzitu neoprávněného zásahu do autorských práv, tedy počet a rozsah dílčích útoků
* dobu trvání protiprávního jednání
* charakter předmětů ochrany, do jejichž práv bylo neoprávněně zasaženo
* dále i osobu pachatele,
* míru zavinění a jeho pohnutku,
* význam chráněného zájmu, který byl činem dotčen,
* způsob provedení činu a jeho následky a okolnosti, za kterých byl čin spáchán,

a rozhodne, zda se v konkrétním případě jedná o **zločin**, **přečin** či „pouze“ o **přestupek**. V souladu s platnou právní terminologií se fyzické osoby dopouští přestupku zatímco právnické osoby a podnikající fyzické osoby správního deliktu.

[**TRESTNĚPRÁVNÍ ODPOVĚDNOST:**](http://www.cpufilm.cz/new/www/trestnepravniodpovednost.html) Jakékoliv neoprávněné užití díla, uměleckého výkonu, zvukového či obrazově - zvukového záznamu nebo vysílání rozhlasu nebo televize, ke kterému nedal oprávněný subjekt svolení, je sice protiprávní, nemusí se však automaticky jednat o trestný čin porušení autorského práva, práv souvisejících s právem s práv k databázi podle § 270 trestního zákoníku. To posoudí s přihlédnutím ke konkrétním okolnostem případu vyšetřující policejní orgán ve spolupráci se státním zástupcem. Trestní sazba trestného činu dle § 270 trestního zákoníku umožňuje uložit trest odnětí svobody až na dvě léta, peněžitý trest až do 36,5 milionu korun nebo trest propadnutí věci nebo jiné majetkové hodnoty. Pokud se pachatel dopustí činu ve **značném** **rozsahu** nebo jím získá **značný** **prospěch**, trestní sazba je vyšší a soud tak může uložit trest odnětí svobody na šest měsíců až pět let, peněžitý trest nebo trest propadnutí věci nebo jiné majetkové hodnoty, a v případě získání prospěchu velkého rozsahu nebo způsobení škody velkého rozsahu hrozí pachateli trest odnětí svobody na tři až osm let. Trestní sazba však pouze definuje výměry trestů stanovených za určité trestné činy trestním zákoníkem. V daném případě rozhodne až soud, jaký vůbec a jak vysoký trest v rámci zákonem stanovené trestní sazby uloží s přihlédnutím ke konkrétním okolnostem případu.

~~K výkladu § 270 tr. zákoníku, resp. § 152 dříve účinného tr. zákona, upozorňujeme na usnesení Nejvyššího soudu ČR k výkladu znaků trestného činu porušování autorského práva podle § 152 tr. zák., sp. zn. 2 Tzn 46/96 ze dne 17.7.1996, v jehož odůvodnění se konstatuje, že "ustanovení § 152 tr. zák. je tzv. normou blanketní, která odkazuje předpisy o právu autorském.~~ Z hlediska posuzování subjektivní stránky jednání pachatele tohoto trestného činu proto platí, že neznalost autorského zákona se posuzuje stejně, jako neznalost normy trestní a pachatele proto nevyviňuje."

**ZA PIRÁTSTVÍ TEDY HROZÍ:**

1. především povinnost nahradit způsobenou škodu a vydat bezdůvodné obohacení (občanskoprávní odpovědnost, možno požadovat i v trestním řízení);
2. pokuta až 150 000,– Kč (přestupková odpovědnost);
3. trest odnětí svobody až na dva roky; případně šest měsíců až pět let, získal-li pachatel činem **značný** **prospěch** nebo dopustil-li se takového činu ve **značném** **rozsahu**, a v případě získání prospěchu velkého rozsahu nebo způsobení škody velkého rozsahu tři až osm let; peněžitý trest až do 36 a půl milionu korun; trest propadnutí věci – počítače, kamery, kopií filmu atd. (trestněprávní odpovědnost). Návodce, pomocník a organizátor trestného činu jsou trestně odpovědní stejně jako pachatel, a může jim být uložen stejný trest.

[**ODPOVĚDNOST DĚTÍ A MLADISTVÝCH:**](http://www.cpufilm.cz/new/www/mladistvi.html)**HROZÍ TREST I DÍTĚTI MLADŠÍMU 15 LET?**  
Dítě mladší 15 let není trestně odpovědné, dopustí-li se však činu jinak trestného, učiní soud pro mládež opatření potřebná k jeho nápravě. Soud pro mládež může dítěti uložit:

* dohled probačního úředníka
* zařazení do vhodného výchovného programu

I takové dítě je však odpovědné za škodu, kterou způsobilo, a musí ji uhradit buď samo, nebo s pomocí svých rodičů. Musí vydat i zisk, který protiprávní činností získalo.

**JAKÝ TREST HROZÍ MLADISTVÉMU?**  
Pirátství je protiprávní, obecně se jedná o trestný čin porušení autorského práva podle § 270 trestního zákoníku. Trestný čin spáchaný mladistvým (tedy osobou ve věku 15–18 let) se označuje jako provinění. Soud pro mládež může mladistvému uložit:

1. trestní opatření

* obecně prospěšné práce
* peněžité opatření až do výše 1.8M Kč
* propadnutí věci nebo jiné majetkové hodnoty, a to nejen pirátských kopií, ale i zařízení sloužícího k jejich výrobě (CD či DVD vypalovačka, počítač, nosiče) a veškerého zisku
* zákaz činnosti
* vyhoštění, jedná-li se o cizince
* domácí vězení
* zákaz vstupu na sportovní, kulturní nebo jiné společenské akce
* odnětí svobody až na polovinu doby jako dospělému, tedy na jeden rok, 2 a půl roku nebo 4 léta

1. výchovná opatření

* dohled probačního úředníka nebo probační program (výchovný)
* výchovné povinnosti či výchovná omezení
* napomenutí s výstrahou

1. ochranné opatření

* zabrání věci nebo jiné majetkové hodnoty
* ochranná výchova

1. povinnost k náhradě způsobené škody a vydání bezdůvodného obohacení

**Správny delikt (všeobecne)** – označenie pre všetky verejnoprávne delikty, ktoré spracováva správny úrad. Delikt – porušenie práva alebo ním stanovenej povinnosti

- **Priestupok/správny delikt podľa §105a a 105b** – Autorský zákon , osoba sa dopustí priestupku tým, že:

* **neoprávnene použije** autorské dielo, umelecký výkon, zvykový, či zvukovo-obrazový záznam, rozhlasové alebo televízne vysielanie... (pokuta až 150 000 Kč)
* **neoprávnene zasahuje do autorského práva** (pokuta 100 000 Kč)
* ako obchodník, ktorý sa zúčastňuje predaja originálov umeleckého diela, **nesplní oznamovaciu povinnosť** (pokuta 50 000 Kč)

- **Príklady**: výroba a rozširovanie kópií DVD filmov (pre vlastnú potrebu je to ok), zdieľanie cez torrent, neoprávnené verejné premietanie filmov – v autobuse, lietadle, klube – bez oprávnenie

**2)Elektronický podpis a elektronická pečeť – právní úprava a druhy**

**Aktuálne platia:**

* Aktuálne platí Zákon č. 250/2017 Sb. *Zákon o elektronické identifikaci*
* Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (eIDAS)

**eIDAS – electronic identification and services**

- Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES

- Zveřejněno v Úředním věstníku EU dne 28. 8. 2014

**Cíle nařízení eIDAS?**

* Jeden z důležitých nástrojů pro dotvoření digitálního volného vnitřního trhu
* Zvýšení důvěryhodnosti elektronických transakcí v rámci vnitřního trhu
* Vytvoření jednotného rámce pro elektronickou identifikaci jednotlivých subjektů - společný základ pro elektronickou komunikaci mezi občany, podniky a orgány veřejné moci pro efektivnost veřejných a soukromých on-line služeb, elektronického podnikání a elektronického obchodu (obecně dopadá do veřejného i soukromého práva!)
* Nahrazení současné evropské legislativy pro elektronické podpisy a rozšíření působnosti oproti původní směrnici

**Proč forma nařízení?**

* Nařízení je závazné a přímo použitelné ve všech členských státech
* Nahrazení původní směrnice Evropského parlamentu a Rady 1999/93/ES ze dne   
  13. prosince 1999 o zásadách Společenství pro elektronické podpisy

**Elektronický podpis dle čl. 3/10 eidas**

* data v elektronické podobě,
* která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena
* a která podepisující osoba používá k podepsání
* **Zaručený elektronický podpis umožňuje jednoznačnou identifikaci podepisující osoby**

**ČL. 25 EIDAS**

1. Elektronickému podpisu nesmějí být upírány právní účinky a nesmí být odmítán jako důkaz v soudním a správním řízení pouze z toho důvodu, že má elektronickou podobu nebo že nesplňuje požadavky na kvalifikované elektronické podpisy.
2. Kvalifikovaný elektronický podpis má právní účinek rovnocenný vlastnoručnímu podpisu.
3. Kvalifikovaný elektronický podpis založený na kvalifikovaném certifikátu vydaném v jednom členském státě se uznává jako kvalifikovaný elektronický podpis ve všech ostatních členských státech.



**Druhy elektronických podpisov podla eIDAS:**

* **elektronický podpis** - cokoli, co nějakým způsobem identifikuje subjekt a je připojeno k jiným datům
* **zaručený elektronický podpis** - je založen na certifikátu, ale na ten nejsou kladeny žádné požadavky – může jít i o testovací certifikát (ten může obsahovat jakoukoli informaci)
* **kvalifikovaný elektronický podpis** - musí být založen na kvalifikovaném certifikátu pro elektronický podpis a musí být vytvořen pomocí kvalifikovaného prostředku pro vytváření elektronických podpisů (např. čipové karty – eID nebo tokeny)

**Zaručený elektronický podpis – čl. 26**

-musí splňovat tyto požadavky:

* je jednoznačně spojen s podepisující osobou
* umožňuje identifikaci podepisující osoby
* je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou
* je k datům, která jsou tímto podpisem podepsána, připojen takovým způsobem, že je možné zjistit jakoukoliv následnou změnu dat. (digitalny podpis, hash)

**Kvalifikovaný elektronický podpis**

-Kvalifikovaný (eIDAS) = uznávaný (starý zákon o el. Podpisu)

-Čl. 28 a násl. nařízení eIDAS

-musí splňovat:

* Kvalifikované certifikáty
* Požadavky kladené na certifikáty
* Certifikace a postupy
* Zveřejnění seznamu certifikačních prostředků
* Požadavky na ověřování certifikátu
* kvalifikovaná služba ověřování platnosti kvalifikovaných elektronických podpisů
* kvalifikovaná služba uchovávání kvalifikovaných elektronických podpisů

**Návrh novely zákona o občanských průkazech**

– zavede jednotné občanské průkazy s čipem v průběhu roku 2018

– na občanském průkazu s čipem bude v I.etapě identifikační certifikát občanského průkazu a v II. etapě kvalifikovaný podpis na kvalifikovaném certifikátu držitele občanského průkazu

– občanský průkaz s čipem bude QSCD(Zariadenia pre podpis a pečať) pro vytváření elektronických podpisů

– občanský průkaz s čipem bude bezplatně vydáván

# **Zákon č. 250/2017 Sb.*Zákon o elektronické identifikaci***

Schválený zákon zavádí „národní bod pro identifikaci a autentizaci“, což je informační systém, který poskytne formou sdílené služby všem orgánům veřejné moci jednoduchý nástroj k ověření totožnosti uživatelů jejich online služeb. K němu se pak díky zákonu budou moci připojit i soukromoprávní poskytovatelé identitních prostředků, kteří projdou procesem akreditace. Prostředkem s nejvyšší úrovní důvěry (definované nařízením eIDAS) poskytovaným státem pak budou občanské průkazy s čipem a identifikačním certifikátem

**Elektronické pečetě**

-mohou vytvářet (právě a pouze) právnické osoby (zahrnující i organizační složky státu).

-v případě elektronické pecete nejde o projev vůle, ale o **vyjádření** **původu**

Elektronickou pečeť může vytvářet jen **právnická** osoba (včetně organizační složky státu) – a může ji připojit jen na to, čeho je sama **původcem**.

Zjednodušeně: el. pečeť může přidat jen na „něco svého“, a nikoli na „něco cizího“. Důvodem je  skutečnost, že nejde o projev vůle (v právním slova smyslu),

Takže třeba smlouvu v elektronické podobě (či žalobu k soudu apod.) pomocí elektronické pečeti nestvrdíte, ani kdyby jednající stranou byla právnická osoba. K tomu musí být fyzická osoba, a ta musí k podepsání smlouvy použít svůj elektronický podpis.

**3) Datové schránky – právní úprava a praxe používání**

**Datové schránky**

Vzájemné doručování úředních dokumentů v papírové podobě se v České republice stalo od 1. července 2009 z velké části minulostí. V účinnost vstoupil nový zákon č. 300/2008 Sb. o elektronických úkonech a autorizované konverzi dokumentů (dále jen „zákon“). Ten fakticky zrovnoprávnil elektronickou a papírovou formu komunikace, a to prostřednictvím tzv. datových schránek. Povinně je ze zákona musí používat nejen veškeré **Orgány veřejné moci (dále jen „OVM“),** kterým tuto povinnost elektronické komunikace zákon ukládá, ale i právnické osoby. Fyzickým osobám (a to i nepodnikajícím) dává zákon možnost volby - chtějí-li si komunikaci zjednodušit, usnadnit a zlevnit, mohou si datovou schránku nechat zřídit na vlastní žádost.

Správcem informačního systému datových schránek je Ministerstvo vnitra ČR (dále jen „ministerstvo“) a provozovatelem Česká pošta s.p., která zajišťuje provoz celého systému, rozesílá přístupové údaje apod.

**Co je datová schránka?**

Datová schránka je elektronické úložiště, které je určeno:

* k doručování OVM
* k provádění úkonů vůči OVM
* k dodávání dokumentů fyzických osob, podnikajících fyzických osob a právnických osob.

**POZOR - MĚLI BYSTE VĚDĚT**

Datová schránka není obdobou e-mailu (který na rozdíl od datové schránky negarantuje doručení přenášené zprávy adresátovi a jednoznačnou identifikaci odesílatele a adresáta) a neslouží k dlouhodobé archivaci tzv. datových zpráv. Datové zprávy jsou v datové schránce standardně uloženy maximálně po dobu 90 dnů ode dne jejich doručení adresátovi.

**Pro koho jsou datové schránky zřizovány?**

Povinně je mají zřízeny:

* OVM
* právnické osoby zřízené zákonem
* právnické osoby zapsané v obchodním rejstříku (obchodní společnosti a družstva)
* organizační složky podniku zahraniční právnické osoby zapsané v obchodním rejstříku
* insolvenční správci, advokáti, daňoví poradci

**Na žádost se zřizují:**

* fyzickým osobám
* fyzickým osobám podnikajícím
* právnickým osobám, které se nezapisují do obchodního rejstříku (spolky, nadace, ústavy)

**Zřizovány jsou tedy 4 různé typy datových schránek:**

* Datové schránky OVM (mezi něž patří státní orgány, orgány územně samosprávných celků, notáři, soudní exekutoři, zdravotní pojišťovny, samosprávné komory atd.),
* právnických osob,
* fyzických osob
* fyzických osob podnikajících.

Vykonává-li fyzická nebo právnická osoba působnost v oblasti veřejné správy, ministerstvo jí na žádost umožní, aby její datová schránka plnila rovněž funkci datové schránky OVM.

**Princip doručování a odesílání datových zpráv**

Účelem zavedení a spuštění systému datových schránek bylo vytvoření systému, prostřednictvím kterého mohou orgány veřejné moci efektivně, zabezpečeně, garantovaně a rychle komunikovat 5 jednak samy se sebou, a rovněž tak s adresáty veřejné správy (firmami a občany). Datové zprávy dodávané prostřednictvím informačního systému datových schránek jsou doručovány ve stejném právním režimu jako doporučené zásilky doručované prostřednictvím držitele poštovní licence. To samé platí i pro zásilky, které jsou doručovány do vlastních rukou adresáta.

**Povinnost komunikovat prostřednictvím datových schránek mají:**

* OVM mezi sebou navzájem, pokud to povaha dokumentu umožňuje a nedoručuje-li se na místě.
* OVM vůči subjektům, které mají datovou schránku zřízenou a zpřístupněnou, pokud to povaha dokumentu umožňuje a nedoručuje-li se na místě nebo veřejnou vyhláškou. Má-li daný subjekt zpřístupněnou datovou schránku.

**Dobrovolnou komunikaci prostřednictvím datových schránek mají:**

* Subjekty, které mají datovou schránku zřízenou a zpřístupněnou vůči OVM, pokud to povaha dokumentu umožňuje, má-li daný subjekt zpřístupněnou datovou schránku - úkon má účinky písemného a podepsaného podání.
* Subjekty, které mají datovou schránku zřízenou a zpřístupněnou a chtějí mezi sebou komunikovat navzájem (tzv. business-to-business komunikace, dále jen „B2B“), pokud to povaha dokumentu umožňuje, má-li daný subjekt zpřístupněnou datovou schránku, příjemce si přijímání zpráv povolí ve své datové schránce a odesílatel si službu aktivuje prostřednictvím klientské zóny na http://www.cpost.cz u držitele poštovní licence.

Výchozím předpokladem pro zasílání datových zpráv je nutnost přikládání příloh ve stanoveném formátu (docx, xlsx, pptx, tif, edi).

**Kdy OVM považuje dokument za doručený danému adresátovi veřejné správy?**

* Přihlásí-li se do davové schránky oprávněná osoba, pověřená osoba, administrátor či elektronický systém umožňující dálkové napojení na informační systém datových schránek (zpravidla se jedná o spisovou službu apod.).
* Posledním dnem, kdy marně uplyne 10 - denní lhůta pro vyzvednutí dodané datové zprávy (jedná se o takzvané doručení fikcí).

**Kdy adresát veřejné správy považuje dokument za doručený danému OVM?**

* Okamžikem, kdy je datová zpráva dodána do datové schránky OVM

**Kdy se dokument považuje za doručený v režimu B2B?**

* Dodaný dokument do datové schránky adresáta se považuje za doručený okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k tomuto dokumentu. Tato komunikace je držitelem poštovní licence zpoplatněna.

V určitých případech (dlouhodobá nemoc, dočasné znepřístupnění datové schránky pro oprávněnou osobu, které nezavinila) se lze z objektivních důvodů domáhat neúčinnosti doručení, a to u OVM, jenž danou datovou zprávu adresátovi zaslal. 6 Datové zprávy zasílané prostřednictvím datových stránek k OVM nemusí být primárně opatřeny zaručeným elektronickým podpisem. Dle § 18, odst. 2) zákona, totiž úkon učiněný prostřednictvím datové schránky vůči OVM má stejné účinky jako úkon učiněný písemně a podepsaný, ledaže jiný právní předpis nebo vnitřní předpis požaduje společný úkon více z uvedených osob.

**Praktické aspekty používání datové schránky**

-Mezi největší výhody používání datových schránek patří:

* jednoznačná identifikace odesílatele a adresáta
* vysoká efektivita komunikace
* úspora finančních prostředků
* úspora času při doručování
* garantovaná vysoká spolehlivost a zaručená bezpečnost při doručování
* v porovnání s klasickým doručováním zaručuje nadstandardní dostupnost 24h/7dnů a využitelnost služby z kteréhokoliv místa, kde je dostupný internet
* povinně ji mají zřízenou všechny OVM
* od 1. 7. 2010 je umožněno neomezené dodávání dokumentů prostřednictvím datových schránek tzv. komunikace B2B

Komunikace s OVM tak může být výrazně rychlejší, jednodušší a z dlouhodobého hlediska daleko méně finančně nákladná než klasické zasílání listovních zásilek, a to již jenom z toho důvodu, že valná většina dokumentů v dnešní době primárně vzniká v elektronické podobě a následně se tiskem převádí do podoby papírové. Tento mezikrok tedy při používání datových schránek zcela odpadá, samozřejmě včetně vynaložení finančních nákladů na něj. Orgány veřejné moci, s nimiž lze komunikovat prostřednictvím datové schránky:

* státní orgány (ministerstvy, Českým statistickým úřadem)
* orgány územně samosprávných celků (obcemi, kraji)
* státní fondy
* zdravotní pojišťovny (VZP, VOZP, ZPMČR)
* Český rozhlas a Česká televize
* samosprávné komory zřízené dle zákona (ČAK, ČLK)
* Česká správa sociálního zabezpečení
* notáři
* soudní exekutoři
* Policie ČR
* a další.

<http://www.ohkmb.cz/datove-schranky.pdf>

**4) Provozní a lokalizační údaje a jejich využití v trestním řízení**

**Prevádzkové údaje** = akékoľvek údaje spracovávané pre potrebu prenosu správy sieťou elektronickej komunikácie, alebo pri jej účtovaní (§90 ZEK)

**Lokalizačné údaje** = akékoľvek údaje spracovávané v sieti elektronickej komunikácie, ktoré určujú zemepisnú polohu koncového zariadenia užívateľa verejne dostupnej služby elektronických komunikácií (§91 ZEK – zákon o elektronických komunikáciách)

- Povinné subjekty (mobilný operátori, poskytovatelia internetu a pod.) musia podľa ZEK(Zákon o elektronických komnikacích) uchovávať prevádzkové a lokalizačné údaje podľa §93 odst. 3 ZEK po dobu 6 mesiacov – pre prístup k týmto údajom je nutné povolenie podľa §88A TR od štátneho zástupcu

- Nepovinné subjekty logicky nemusia uchovávať tieto údaje

## Popište rozdíly v modu přístupu k provozním a lokalizačním údajům pro subjekty řídící se zákonem o elektronických komunikacích a pro subjekty, které se tímto zákonem neřídí.

Provozní a lokalizační údaje (6 měsíců) – Platí pro subjekty dle ZEK – mimo ZEK se nevztahuje a uchovávání není nutné. ([ZEK § 91](http://zakony.centrum.cz/zakon-o-elektronickych-komunikacich/cast-1-hlava-5-dil-1-paragraf-91))

**(1)** Lokalizačními údaji se rozumí jakékoli údaje zpracovávané v síti elektronických komunikací nebo službou elektronických komunikací, které určují zeměpisnou polohu telekomunikačního koncového zařízení uživatele veřejně dostupné služby elektronických komunikací.

**(2)** Provádí-li podnikatel zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací zpracování lokalizačních údajů jiných než provozních, které se vztahují k uživateli nebo účastníku, musí tyto údaje učinit anonymními nebo získat souhlas uživatele nebo účastníka se zpracováním....

Metadata – IP adresa jako identifikátor stroje – nepřímý důkaz

BTS, určení polohy apod.

Nelze použít § 8 (Součinnost)

[**Historie uchovávání lokalizačních dat**](http://www.earchiv.cz/i_retention.php3)

Trestní řád donedávna obsahoval i možnost vyžádání si provozních a lokalizačních údajů od poskytovatelů, telekomunikačních operátorů.

Tyto informace měly být poskytnuty soudci a v přípravném řízení státnímu zástupci nebo policejnímu orgánu. Ústavní soud však toto ustanovení svými nálezy zrušilo, protože nekladlo dostatečné záruky pro ochranu práva na soukromí.

Byly zde neurčité podmínky využitelnosti údajů pro trestní řízení, chybějící vymezení trestných činů, při jejichž stíhání lze data použít. To vedlo z nárůstu žádostí o tyto informace a zároveň tedy i k zásahu do základních práv.

Ústavní soud zrušil poskytování provozních a lokalizačních údajů dvěma kroky. Nejdříve v březnu roku 2011 zrušil povinnost telekomunikačních operátorů uchovávat tyto údaje a poté na konci stejného roku zrušil možnost vyžádaní těchto údajů úplně.

Současnost

Zákon o elektronických komunikacích tedy upravuje způsob uchovávání provozních a lokalizačních údajů a vymezuje okruh subjektů, které k nim mohou mít přístup při splnění dalších podmínek. Právě tyto podmínky, za kterých uvedené subjekty mohou získat přístup k uchovaným údajům, upravují další zákony, konkrétně zákon č. 141/1963 Sb., trestní řád, zákon č. 273/2008 Sb., o Policii ČR, zákon č. 154/1994 Sb., o Bezpečnostní informační službě, zákon č. 289/2005 Sb., o Vojenském zpravodajství, a zákon č. 15/1998 Sb., o dohledu v oblasti kapitálového trhu.

**~~Odposlech a záznam zpráv - zákon č. 127/2005 Sb(ZEK)~~**

**~~§ 97 odstavec 3~~**

~~Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu~~ **~~6 měsíců~~** ~~provozní a lokalizační údaje, které jsou vytvářeny nebo zpracovávány při zajišťování jejích veřejných komunikačních sítí a při poskytovávání jejích veřejně dostupných služeb elektronických komunikací~~[**~~)~~**](https://www.zakonyprolidi.cz/cs/2005-127#f2917859)~~. Provozní a lokalizační údaje týkající se neúspěšných pokusů o volání je právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací povinna uchovávat pouze tehdy, jsou-li tyto údaje vytvářeny nebo zpracovávány a zároveň uchovávány nebo zaznamenávány. Současně je tato právnická nebo fyzická osoba povinna zajistit, aby při plnění povinnosti podle věty první a druhé~~ **~~nebyl~~****~~uchováván obsah zpráv~~** ~~a takto uchovávaný dále předáván. Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout~~

**~~a)~~**~~orgánům činným v trestním řízení pro účely a při splnění podmínek stanovených zvláštním právním předpisem~~[**~~)~~**](https://www.zakonyprolidi.cz/cs/2005-127#f4766466)~~,~~

**~~b)~~**~~Policii České republiky pro účely zahájeného pátrání po konkrétní hledané nebo pohřešované osobě, zjištění totožnosti osoby neznámé totožnosti nebo totožnosti nalezené mrtvoly, předcházení nebo odhalování konkrétních hrozeb v oblasti terorismu nebo prověřování chráněné osoby a při splnění podmínek stanovených zvláštním právním předpisem~~[**~~)~~**](https://www.zakonyprolidi.cz/cs/2005-127#f4766467)~~,~~

**~~c)~~**~~Bezpečnostní informační službě pro účely a při splnění podmínek stanovených zvláštním právním předpisem~~[**~~)~~**](https://www.zakonyprolidi.cz/cs/2005-127#f2917856)~~,~~

**~~d)~~**~~Vojenskému zpravodajství pro účely a při splnění podmínek stanovených zvláštním právním předpisem~~[**~~)~~**](https://www.zakonyprolidi.cz/cs/2005-127#f2917858)~~,~~

**~~e)~~**~~České národní bance pro účely a při splnění podmínek stanovených zvláštním právním předpisem~~[**~~)~~**](https://www.zakonyprolidi.cz/cs/2005-127#f4766468)~~.~~

~~Po uplynutí doby podle věty první je právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, povinna je~~ **~~zlikvidovat~~**~~, pokud nebyly poskytnuty orgánům oprávněným k jejich využívání podle zvláštního právního předpisu, nebyl vydán příkaz k jejich uchování podle zvláštního právního předpisu) nebo pokud tento zákon nestanoví jinak (§ 90).~~

**Ochrana osobních, provozních a lokalizačních údajů a důvěrnost komunikací**

**§ 88a (1)** Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna zajistit, aby provozní a lokalizační údaje uchovávané podle § 97 odst. 3 měly stejnou kvalitu a podléhaly stejnému zabezpečení a ochraně před neoprávněným přístupem, změnou, zničením, ztrátou anebo odcizením nebo jiným neoprávněným zpracováním nebo využitím, jako údaje podle § 88; tímto nejsou dotčeny povinnosti stanovené zvláštním právním předpisem 34).

* § 78 Povinnost k vydání věci
* § 88 Odposlech
* § 88a Záznam telekomunikačního provozu
* § 158d Sledování osob a věcí

**ROZDÍLY**

Poskytování provozních a lokalizačních údajů na vyžádání není po rozhodnutí ústavního soudu v roce 2011 možné.

**Podle § 97 (3)** - Právnická nebo fyzická osoba, která provozní a lokalizační údaje uchovává, je na požádání povinna je bezodkladně poskytnout:

1. orgánům činným v trestním řízení
2. Policii České republiky
3. Bezpečnostní informační službě
4. Vojenskému zpravodajství
5. České národní bance

**Data retention**

- data(local a prvoz) by sa podľa EU smernice nemali uchovávať s výnimkou článku 15 kedy sa môžmu uchovávať keď je to vzájmu národní bezpečnosti(vtedy si to mohli štáty implementovať), potom bola ďalšia smernica, ktorá prikazovala zavedenie uchovávania, ústavný súd ČR nariadil upravenie zákona o elektrických komunukáciach paragraaf 97 článok 3 a 4 (na vymedzenie orgánov ktoré s tým možu pracovať),neskôr EU zistila,že je to v rozpore s chartou, tak sa to zrušilo. Väčšina členských štatov si uchovávanie zrušilo ale v ČR ostalo na základe 1. Smernice podľa ćlánku 15(národná bezpečnosť). V roku 2016 ustavný súd vydal rozhodnutie že česká úprava poľa prvej smernice EU. Zle si vyložili článok 15 a úprava nemôže podľa tej smernice existovať. V súčastnej dobe je to v ČR zavedené ale je to v rozpore s EU smernicou(tou prvou -ePrivacy)

* **2006 - Směrnice Evropského parlamentua Rady 2006/24/ES** o **uchování údajů vytvářených nebo zpracovávaných v souvislosti s poskytováním veřejně dostupných služeb elektronických komunikací nebo veřejných komunikačních sítí**
* Zajištění dostupnosti údajů pro vyšetřování, stíhání trestných činů
* stížnosti: neproporciální zásah do **soukromí**, permanentní **sledovaní všech**, **absence podezření**, porušení zákonů (nedotknutelnost soukromí, telekomunikační tajemství …)
* **rozhodnutí ÚS**: ponechává České republice dostatečný prostor pro její ústavně konformní transpozici do domácího právního řádu ALE nejasné vymezení orgánů, nedostatečné záruky
* úpravy:
  + Taxativní výčet oprávněných orgánů
  + Povinnost zlikvidovat data neobnovitelným způsobem
* spor o poskytovatele veřejných wi-fi
* **2014 -** EÚ zistila rozpory s **Chartou základních práv** (čl. 7 a 8)🡪**zrušenie smernice vo väčšine štátov** (Rakúsko - 2014, Slovensko -2015)
* Dôsledok zrušenia
  + **nie je povinnosť uchovávať DR**
  + pôvodné opatrenie nespĺňalo nové podmienky (**čo platilo podľa starej smernice bolo protiprávne**)
* **V ČR sa zatiaľ nevie či sa zruší, stále sa čaká na rozhodnutie ústavného súdu**

**ZEK se řídí:**

Právnická nebo fyzická osoba zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací je povinna uchovávat po dobu 6 měsíců provozní a lokalizační údaje…

**5) Právo elektronických komunikací – předmět a účel právní úpravy**

**-Zákon č. 127/2005 Sb.**

**Oblast regulace - definice**

* Upravuje služby elektronických komunikací (§2 písm. n) ZoEK) = obvykle za úplatu, spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací(telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize)
  + Vyjma služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací
* Síť elektronických komunikací (§2 písm. h) ZoEK) = přenosové systémy , které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace
* Obsah komunikace není předmětem úpravy

### **§ 4 CÍLE A ZÁKLADNÍ ZÁSADY REGULACE**

Regulace je prováděna za účelem nahradit chybějící účinky hospodářské soutěže, vytvářet předpoklady pro řádné fungování hospodářské soutěže a pro ochranu uživatelů a dalších účastníků trhu do doby dosažení plně konkurenčního prostředí.

**Regulácia**

- je všeobecne súbor právnych nástrojov daných štátom, ktoré ovplyvňujú/obmedzujú aktivitu ľudí

- **regulujú sa služby a siete** (obsah nie)

**Účel regulace**

* vytvorenie a ochrana trhu elektronických komunikácií (ex ante) - reguláciou sa udržiava otvorený trh – umožňuje prístup na trh - v elektronických komunikáciách je ochrana trhu trochu iná ako všeobecná úprava ochrany hospodárskej súťaže (ex post)
* Ochrana uživatele - spotřebitele
* Univerzální služba
* Modernizace infrastruktury
* Síťová neutralita
* Ochrana soukromí a osobních údajů

**6) Síťová neutralita v EU a USA**

**Princíp sieťovej neutrality** je veľmi jednoduchý. Všetok obsah šírený na internete má byť z pohľadu poskytovateľov pripojenia (ISP) **rovnoprávny**. Takže operátori pevného aj mobilného pripojenia **nesmú** nijako **odlišovať**, či sa cez ich siete do obývačiek a do firiem dostáva streamované video z Netflixu alebo webová stránka malého e-shopu.

[**Zrušenie sieťovej**](https://www.wired.com/story/after-fcc-vote-net-neutrality-fight-moves-to-courts-congress/)**neutrality** teraz v USA dalo poskytovateľom internetu možnosť určovať, aký obsah dovolia prenášať cez ich siete, respektíve akou rýchlosťou. Bude legálne, že napríklad všetok obsah zo služby Spotify nebudú cez ich pripojenie šíriť, pretože sami poskytujú konkurenčnú streamovaciu hudobnú službu. Respektíve budú pripojenie na Spotify spomaľovať.

K uzneseniu FCC **sa**[**oficiálne vyjadrili**](https://techcrunch.com/gallery/what-telecoms-and-tech-companies-are-saying-about-the-fccs-net-neutrality-decision/) najväčší internetoví hráči. Sprostredkovatelia obsahu ako Google, Twitter, Microsoft, Netflix, Amazon, Facebook alebo Airbnb odsúdili tento čin a vyjadrili sklamanie. Ostávajú zástancami internetovej neutrality.

Hlavný argument šéfa FCC Ajita Paia pre prijatie nových opatrení - **zlepšiť podmienky pre rozvoj** infraštruktúry, a teda **rozširovanie** **pokrytia** internetovým signálom aj do odľahlejších a chudobnejších oblastí.

**Vyjádření Českého telekomunikačního úřadu k vybraným otázkám přístupu k otevřenému internetu a evropským pravidlům síťové neutrality**

Zdroj: <https://www.ctu.cz/sites/default/files/obsah/stranky/956/soubory/vyjadreniceskehotelekomunikacnihouradukvybranymotazkampristupukotevrenemuinternetuaevropskympravidlu.pdf>

**I. Úvod**

Dne 25. listopadu 2015 bylo schváleno Nařízení Evropského parlamentu a Rady (EU) 2015/2120, kterým se stanoví opatření týkající se přístupu k otevřenému internetu a mění směrnice 2002/22/ES o univerzální službě a právech uživatelů týkajících se sítí a služeb elektronických komunikací a nařízení (EU) č. 531/2012 o roamingu ve veřejných mobilních komunikačních sítích v Unii (dále jen „Nařízení“), které stanovuje mj. společná pravidla pro zajištění rovného a nediskriminačního nakládání s provozem při poskytování služeb přístupu k internetu a zajištění souvisejících práv koncových uživatelů. Nařízení dále v článku 5 pověřuje sdružení BEREC vydáním Pokynů pro provádění povinností vnitrostátních regulačních úřadů (dále jen Pokyny) 1 s cílem přispět k jednotnému uplatňování Nařízení. Pokyny byly v souladu s článkem 5 Nařízení vydány k 30. srpnu 2016.

Nařízení se vztahuje na poskytovatele služeb přístupu k internetu a provozovatele sítí elektronických komunikací, kteří jsou podnikateli v elektronických komunikacích ve smyslu zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále jen „Zákon“), při poskytování veřejně dostupné služby přístupu k internetu

**II. Nabízení služeb přístupu k internetu v ČR**

Poskytovatelé přístupu k internetu se obecně snaží zatraktivnit pro koncové uživatele své služby používáním různých obchodních a technických praktik. Úřad uvádí níže na základě reálných zkušeností z fungování trhu v ČR a s přihlédnutím k jeho specifikům případy takových praktik, u nichž posuzoval konkrétní parametry reálně nabízených služeb a k nimž považuje za důležité se v rámci možností daných Nařízením a Pokyny vyjádřit. Přitom je veden snahou zamezit případným výkladovým nejasnostem souvisejícím s kontrolou naplňování požadavků Nařízení v rámci jemu určených kompetencí a napomoci poskytovatelům služeb přístupu k internetu postupovat správně při tvorbě nabídky služeb.

**1. Zero rating**

Obchodní praktika označovaná jako „zero rating“ (dále jen „ZR“) spočívá ve zpoplatnění datových přenosů nulovou nebo jinou než obvykle účtovanou sazbou. V ČR jsou tyto praktiky reálně využívány zejména při poskytování mobilních služeb, které jsou nabízeny s limity pro přenesená data za určité časové období. Úřad bude v případě potřeby či žádosti posuzovat uplatnění ZR individuálně, a to z hlediska souladu s Pokyny s ohledem na cíle Nařízení.

Nejběžnějším typem ZR je nezapočítávání přenosu dat souvisejících s určitou konkrétní aplikací, nebo kategorií aplikací, do datového limitu služby přístupu k internetu, což znamená ve svém důsledku účtování nulové, nebo nižší ceny za takový přenos dat. Tyto praktiky nejsou v obecné rovině zakázány a Úřad je bude v souladu s výše uvedenými principy v případě potřeby posuzovat individuálně, případně stanoví obecnou výjimku.

Další obchodní praktikou je nezpoplatnění veškerého datového přenosu v rámci přístupu k internetu v konkrétních časových úsecích, např. v nočních hodinách, o víkendech apod. Úřad v souladu s bodem 35 Pokynů považuje tuto praktiku za povolenou a zcela v souladu s Nařízením.

Dalším příkladem ZR je praktika, kdy datové přenosy pro potřeby některých aplikací, služeb či konkrétního obsahu fungují i po dosažení datového limitu koncovým uživatelem, zatímco ostatní datové přenosy jsou zastaveny případně zpomaleny. Takový postup obecně není povolen, a pokud není stanovena specifická výjimka (viz níže), je považován za porušení Nařízení článku 3 (3) první a třetí pododstavec, a bod 55 Pokynů.

**Přístup do tzv. samoobsluhy (self-care)**

V obecné rovině platí, že pokud je přenos dat pro konkrétní aplikaci umožněn i po dosažení limitu pro datový přenos, zatímco ostatní provoz je zablokován, nebo zpomalen, jedná se o zakázanou praktiku (viz výše). Přípustnou výjimkou uvedenou v Pokynech (bod 35) tvoří pouze pokračující přenos dat za účelem dokoupení dalších dat. Úřad s ohledem na charakter nabídky služeb přístupu k internetu zejména mobilními operátory a na praxi při využívání služeb považuje za účelné toto ustanovení vztáhnout i na přístup do tzv. samoobsluhy poskytovatele přístupu k internetu, kde si uživatel nastavuje své služby, kontroluje faktury, vyúčtování apod. Prostřednictvím 3 samoobsluhy může též poskytovatel sdělovat svým uživatelům další údaje o jím využívané službě, např. zpřístupňovat smluvní dokumentaci včetně povinně zveřejňovaných informací.

**2. Nabídka služeb přístupu k internetu s limitem datového objemu**

Služby s omezením objemu přenesených dat jsou na trhu v ČR nabízeny převážně v mobilních sítích. Existují nabídky, u nichž je při smluvním omezení v objemu přenesených dat po vyčerpání tohoto objemu služba přístupu k internetu nadále poskytována, avšak se sníženou rychlostí stahování a vkládání dat. Úřad považuje takovou nabídku služby přístupu k internetu za přípustnou, pokud se jedná o snížení rychlosti přenosu dat stejně pro **všechny** aplikace/služby/obsah. Smluvní podmínky musí dle názoru Úřadu obsahovat konkrétní popis toho, jakým způsobem jsou přenesená data započítávána (zda pouze stahovaná data, tj. v jednom směru, nebo obou směrech) a na jaké vrstvě se objem přenesených dat měří. Ve smluvních podmínkách musí být dále jednoznačně stanoveny parametry služby a případná další omezení aplikovaná po vyčerpání datového limitu. Minimální rychlost po vyčerpání smluvně omezeného objemu přenesených dat může být nižší než rychlost při běžném poskytování služby.

**3. Omezování přístupu k obsahu**

V minulosti se na trhu elektronických komunikací objevovaly různé služby nabízející blokování určitého typu obsahu. Jednalo se o blokování reklamy, blokováni nevhodného obsahu formou rodičovských zámků apod. Tyto služby byly v určité formě nabízeny i v ČR. Služba přístupu k internetu je definována v Nařízení a musí být poskytovatelem vždy nabízena a poskytována jako neomezená ve smyslu čl. 3 odst. 1 Nařízení. Od nabytí účinnosti Nařízení může k případnému zabránění přenosu (blokování) byť části obsahu, některých služeb, aplikací či zpráv dojít pouze na koncovém zařízení koncového uživatele, s výjimkami uvedenými v čl. 3 (3) třetí pododstavec Nařízení. Uživatel má tímto možnost přímo a v reálném čase svou volbu realizovat (zapnout či vypnout blokování), a to bez dalšího nutného zásahu poskytovatele služby přístupu k internetu.

**7) Ochrana osobních údajů – vymezení osob a základní principy zpracování osobních údajů**

**Osobný údaj** - akákoľvek informácia týkajúca sa určeného alebo určiteľného subjektu údajov (fyzická osoba) – napríklad rodné číslo, dátum narodenia, identita, zdravotný stav (to je dokonca citlivý osobný údaj)

- osobný údaj je tiež definovaný ako kombinácia osobných aj neosobných údajov, ktorá dokáže stanoviť o akú osobu ide (napr. IP adresa)

**Súkromie** - „právo byť nechaný na pokoji“ (right to be left alone)

* pôvodne bolo chápané priestorovo – napríklad v mojom dome nemá koho zaujímať čo tam robím, čo tam mám
* postupne nabralo aj informačné zložky – nemali by sa odpočúvať telefonáty, správy...
* spadá sem aj právo dobrej povesti – právo na ochranu osobnosti

~~-napr pre fungovanie nejakej appky musia spracovávať iba data ktoré su nezbytné na fungovanie aplikácie, nemôžu spracovávať osobné údaje, ktoré s tým nesúvisia. A nemôžu vyžadovať ich poskytnutie.~~

~~Kombináciou pohlavia, ZIPcodu a data narození sa dá detekovať 87% ameriky~~

**Listina základních práv a svobod**

* Čl. 7 (Ochrana osobnosti a obydlí)
* Čl. 10 (zejména odstavec 3: „Každý má právo na ochranu před neoprávněným shromažďováním, zveřejňováním nebo jiným zneužíváním údajů o své osobě.“)

**Listina základních práv Evropské unie**

Čl. 8 – Ochrana osobních údajů

* Každý má právo na ochranu osobních údajů, které se ho týkají.
* Tyto údaje musí být zpracovány korektně, k přesně stanoveným účelům a na základě souhlasu dotčené osoby nebo na základě jiného oprávněného důvodu stanoveného zákonem. Každý má právo na přístup k údajům, které o něm byly shromážděny, a má právo na jejich opravu.
* Na dodržování těchto pravidel dohlíží nezávislý orgán.

**Podústavní předpisy**

* Smernica o ochrane fyzických osôb pri spracovaní osobných údajov a voľnom pohybe týchto údajov 95/46/EHS do 28.5.2018
* Zákon č. 101/2000 Sb., o ochraně osobních údajů
* Nařízení EU 2016/679 – nariadenie o ochrane fyzických osôb pri spracúvaní osobných údajov a o voľnom pohybe takýchto údajov od 28.5.2018 – GDPR (General data protection regulation)
* Zákon o ochrane osobných údajov a o zmene niektorých zákonov č. 101/2000 Sb.

**Osobný údaj- rozširujúca definícia:**

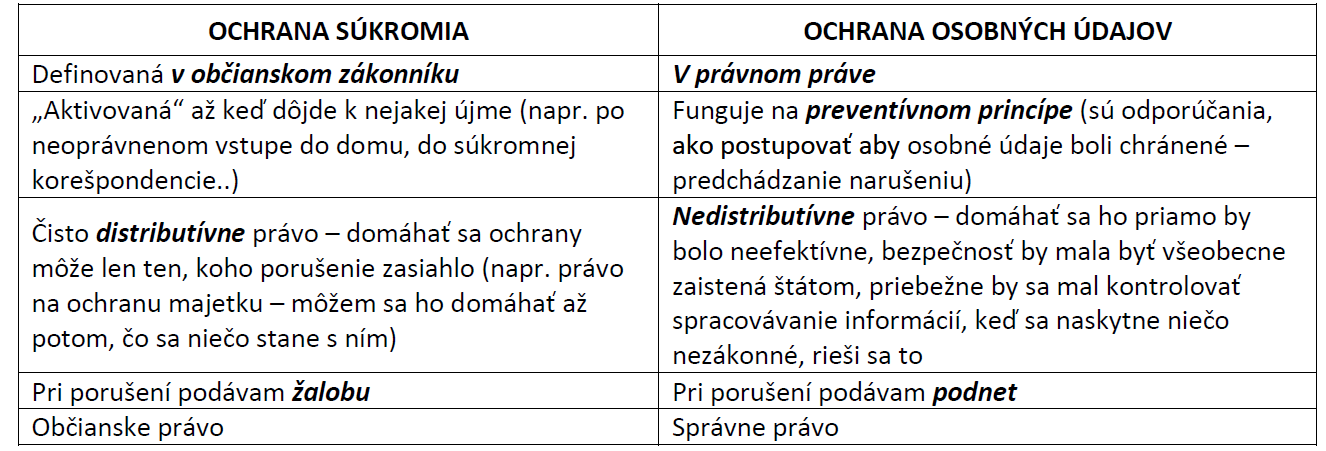
* + Informácia, pomocou ktorej je možné jednoznačne identifikovať subjekt, hlavne na základne čísla, kódu, kombinácii viacerých znakov.
  + Objektívne poňatie: Ak je možné pomocou tohto údaju spárovať človeka aj ilegálnymi prostriedkami, je to osobný údaj. (Judikatúra v Nemecku a novšie rozhodnutia Súdneho dvora Európskej únie (SDEU)
  + Subjektívne poňatie: Ak je možné pomocou tohto údaju spárovať človeka bez neprimeraných nákladov (legálnymi prostriedkami), potom je to osobný údaj. V opačnom prípade to osobný údaj nie je. (Judikatúra ČR, staršie rozhodnutia SDEU)

**Pri narušení súkromia**

- je potrebné podať súkromnoprávnu žalobu na súd. Platia sa náklady na súdne konanie, poškodený je účastníkom konania. Reaktívny účinok – následne až po vykonaní skutku. Týka sa živých a zosnulých fyzických I právnických osôb (šídenie zlého mena)

**Pri podozrení na porušenie ochrany osobných údajov:**

- je možné podať podnet na úrad na ochranu osobných údajov, ten následne zaháji správne konanie a oznamovateľ sa len dozvie výsledok, nie je účastníkom konania. Týka sa len žijucich fyzických osôb.



**Základní principy zpracování osobních údajů**

* **Spracovanie** – zákon 101/2000 Sb. § 4e
* **Operácia** alebo **sústava operácii**, ktoré správca alebo poverený spracovateľ systematicky vykonávajú, a to hlavne automatizovane alebo inými prostriedkami. Sú to prevažne:
  + Zhromažďovanie, ukladanie na nosič informácii, uchovávanie
  + Sprístupňovanie, šírenie, zverejňovanie,
  + vyhľadávanie, úprava, pozmeňovanie, triedenie, kombinovanie
  + blokovanie, likvidácia
* **Zhromažďovanie** OÚ - Postup alebo súbor postupov na získanie údajov, za účelom ich ďalšieho uloženia na nosič informácii pre ich okamžité alebo neskoršie spracovanie
* **Uchovávanie** OÚ - Udržiavanie údajov v podobe, ktorá umožňuje ich ďalšie spracovanie.
* **Blokovanie** OÚ - Operácia alebo sústava operácii, ktorými sa na stanovenú dobu obmedzí spôsob alebo prostriedky spracovania OÚ s výnimkou nevyhnutných zásahov
* **Nutné náležitosti pre spracovanie OÚ:**
  + Informovaný súhlas o spracovaní osobných údajov, ktorý mimo iné musí obsahovať:
    - Právny titul (kdo a v jakém rozsahu může spracovávat údaje)
    - Legálny účel
    - Prostriedky a spôsob spracovania – úkony spracovania
  + Informovaný súhlas – slobodný a vedomý prejav vôle subjektu údajov, ktorého obsahom je súhlas objektu údajov so spracovaním jeho osobných údajov
* **Zabezpečenie** OÚ - správca a spracovateľ sú povinní prijať bezpečnostné opatrenia, aby nemohlo nastať:
  + Neoprávnený alebo náhodný prístup k OÚ, ich zneužitie, zmena, neoprávnený prenos, zničenie či strata
  + Prístup neoprávnenej osoby
  + Počas aj po skončení spracovania
* **Technické opatrenia**:
  + Organizačné poistky
  + Autentizácia a autorizácia prístupu k údajom
  + Zmluvná úprava (Zmluva o mlčanlivosti - NDA – non-disclosure agreement)

**Povinnosti správce**

* Stanovit účel zpracování
* Stanovit prostředky a způsob zpracování
* Zpracovávat pouze přesné osobní údaje
* Shromažďovat údaje pouze za stanoveným účelem a v rozsahu nezbytném pro jeho naplnění
* Shromažďovat údaje otevřeně
* Nesdružovat údaje získané za jinými účely
* Informovat subjekt o zpracování
* (GDPR) Povinnosti vyplývající ze zásady odpovědnosti

**Osobní údaje a jejich zpracování – vymezení a zúčastněné osoby**

* 1. **Zúčastnené osoby:**
  2. ***Správca*** – spracováva dáta, môže delegovať spracovanie dát spracovateľovi
  3. ***Spracovateľ*** – zodpovednosť aj po delegovaní nesie správca; jediná výnimka je ak spracovateľ vedel, že správca porušoval nejaké podmienky ale neupozornil na to
  4. - Spracovávať možno len v rozmedzí na ktoré dal subjekt súhlas
  5. - ***Súhlas*** = jednostranné právne jednanie – dovoľujeme ním tretej osobe, aby nám zasiahla so súkromia

**Fyzická osoba na ktorú sa vzťahujú osobné údaje**

- má právo požiadať správcu údajov o informáciu o spracovaní svojich osobných údajov:

* Účel spracovania,
* kategória OÚ,
* povaha automatizovaného spracovania,
* príjemcovia výsledkov spracovania
* ak je možné predpokladaná doba ochovania
* ak sa osobné údaje nezískali od dotknutej osoby, akékoľvek dostupné informácie, pokiaľ ide o ich zdroj

**Zákon č. 101/2000 Sb. § 5**

**(ods. 1)** **Správce je povinen**

**a)** stanovit účel spracovani osobných údajú

**b)** stanovit prostředky a způsob zpracování osobních údajů,

**c)** zpracovat pouze přesné osobní údaje, které získal v souladu s tímto zákonem. Je-li to nezbytné, osobní údaje aktualizuje.

**d)** shromažďovat osobní údaje odpovídající pouze stanovenému účelu a v rozsahu nezbytném pro naplnění stanového účelu,

**e)** uchovávat osobní údaje pouze po dobu, která je nezbytná k účelu jejich zpracování. Po uplynutí této doby mohou být osobní údaje uchovávány pouze pro účely státní statistické služby, pro účely vědecké a pro účely archivnictví. Při použití pro tyto účely je třeba dbát práva na ochranu před neoprávněným zasahováním do soukromého a osobního života subjektu údajů, a osobní údaje anonymizovat, jakmile je to možné,

**f)** zpracovávat osobní údaje pouze v souladu s účelem, k němuž byly shromážděny. Zpracovávat k jinému účelu lze osobní údaje jen v mezích ustanovení § 3 odst. 6, nebo pokud k tomu dal subjekt údajů předem souhlas,

**g)** shromažďovat osobní údaje pouze otevřeně; je vyloučeno shromažďovat údaje pod záminkou jiného účelu nebo jiné činnosti,

**h)** nesdružovat osobní údaje, které byly získány k rozdílným účelům.

**(ods. 2)** **Správce bez souhlasu může zpracovávat,**

**a)** za účelom dodržení právní povinnosti správce[**)**](https://www.zakonyprolidi.cz/cs/2000-101#f2018410)

**b)** jestliže je to nutné pro plnění

**c)** pokud je to nezbytně třeba k ochraně životně důležitých zájmů subjektu údajů. V tomto případě je třeba bez zbytečného odkladu získat jeho souhlas. Pokud souhlas není dán, musí správce ukončit zpracování a údaje zlikvidovat,

**d)** jedná-li se o oprávněně zveřejněné osobní údaje v souladu se zvláštním právním předpisem.

**e)** pokud je to nezbytné pro ochranu práv a právem chráněných zájmů správce, příjemce nebo jiné dotčené osoby

**f)** pokud poskytuje osobní údaje o veřejně činné osobě, funkcionáři či zaměstnanci veřejné správy, které vypovídají o jeho veřejné anebo úřední činnosti

**g)** jedná-li se o zpracování výlučně pro účely archivnictví podle zvláštního zákona (499/2004 Sb.)

**Teritoriální působnost**

-Článek 4 odst. 1 písm. a) směrnice 95/46 stanoví:

* Každý členský stát použije na zpracování osobních údajů vnitrostátní ustanovení, která přijme na základě této směrnice, pokud:
  + zpracování je prováděno v rámci činností provozovny správce na území členského státu; pokud je stejný správce usazen na území několika členských států, musí přijmout opatření nezbytná pro dodržování povinností stanovených použitelným vnitrostátním právem každou ze svých provozoven“.

- Rozhodnutí SDEU ve věci Google Spain a Weltimmo

-Provozovna = bankovní účet, webová prezentace a stálé právní zastoupení

**GDPR (**[General Data Protection Regulation](https://en.wikipedia.org/wiki/General_Data_Protection_Regulation)**):**

**Základní zásady (GDPR)**

* Osobní údaje musí být ve vztahu k subjektu údajů zpracovávány korektně a zákonným a transparentním způsobem
* Zásada limitace účelem
* Zásada minimalizace údajů (nezbytný rozsah)
* Zásada přesnosti
* Zásada omezení uložení (souvisí s minimalizací; právo být zapomenut)
* Zásada integrity a důvěrnosti
* Zásada odpovědnosti

**Práva subjektu údajů (GDPR)**

* Právo na prístup k osobným údajom
* Právo na opravu osobných údajov
* Právo na vymazanie (zabudnutie)
* Právo na obmedzenie spracovania
* Právo na prenos osobných údajov (ďalšiemu prevádzkovateľovi napr. pri zmene mobil. poskytovateľa)
* Právo namietať spracuvávanie na účely priemého marketing a profilovania

**Princip odpovědnosti (GDPR)**

* Správce má povinnost být schopen kdykoli prokázat, že splňuje zákonné požadavky – nezbytné vedení dokumentace o zpracování
* Záměrná a standardní ochrana osobních údajů (Data protection by design and default)
* Společní správci (čl. 26 GDPR) – nutnost vzájemného ujednání o povinnostech
* Zabezpečení zpracování a hlášení bezpečnostních incident

**Princípy podľa GDPR (general data protection regulation)**

- princíp zodpovednosti správcu za dodržovanie zásad spracovania

* povinnosť viesť záznamy o činnostiach spracovania
* pseudonymizácia (údaje sa nedajú priradiť ku konkrétnej osobe bez doplňujúcich údajov)
* vypracovanie posúdenia vplyvu na ochranu osobných údajov - princíp rizika
* správca musí brať do úvahy kontext, povahu a účel spracovaných osobných údajov a brať do úvahy aj možné riziká, ktoré môžu predstavovať újmu – majetkovú aj nemajetkovú
* zabezpečenie osobných údajov – zamedzenie prístupu neoprávnených osôb, autentizácia a autorizácia pri prístupe k údajom, zmluva o mlčanlivosti

**GDPR – přeshraniční působnost**

Již aktuální případ – Rozhodnutí Google Spain a CNIL

* Čl. 3 odst. 2 -toto nařízení se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí:

1. s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba
2. s monitorováním jejich chování, pokud k němu dochází v rámci Unie.

* Problémy:
  + Vymáhání práva
  + „Všechno nebo nic“

**8) Práva subjektu údajů ve vztahu ke správci a zpracovateli**

**- *Zákon 101/2000 Sb.*** [***§ 12***](https://www.zakonyprolidi.cz/cs/2000-101#f2017883)***,*** [***§ 21***](https://www.zakonyprolidi.cz/cs/2000-101#f2017980)

**§ 12 Přístup subjektu údajů k informacím**

**(1)** Požádá-li subjekt údajů o informaci o zpracování svých osobních údajů, je mu správce povinen tuto informaci bez zbytečného odkladu předat.

**(2)** Obsahem informace je vždy sdělení o

**a)** účelu zpracování osobních údajů,

**b)** osobních údajích, případně kategoriích osobních údajů, které jsou předmětem zpracování, včetně veškerých dostupných informací o jejich zdroji,

**c)** 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,

**d)** příjemci, případně kategoriích příjemců.

**(3)** Správce má právo za poskytnutí informace požadovat přiměřenou úhradu nepřevyšující náklady nezbytné na poskytnutí informace.

**(4)** Povinnost správce poskytnout informace subjektu údajů upravenou v § 12 může za správce plnit zpracovatel.

**§ 21 Ochrana práv subjektů údajů**

**(1)** 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

**a)** požádat správce nebo zpracovatele o vysvětlení,

**b)** požadovat, aby správce nebo zpracovatel odstranil takto vzniklý stav. Zejména se může jednat o blokování, provedení opravy, doplnění nebo likvidaci osobních údajů.

**(2)** Je-li žádost subjektu údajů podle odstavce 1 shledána oprávněnou, správce nebo zpracovatel odstraní neprodleně závadný stav.

**(3)** Pokud vznikla v důsledku zpracování osobních údajů subjektu údajů jiná než majetková újma, postupuje se při uplatňování jejího nároku podle zvláštního zákona.[**)**](https://www.zakonyprolidi.cz/cs/2000-101#f2018434)

**(4)** Došlo-li při zpracování osobních údajů k porušení povinností uložených zákonem u správce nebo u zpracovatele, odpovídají za ně společně a nerozdílně.

**(5)** Správce je povinen bez zbytečného odkladu informovat příjemce o žádosti subjektu údajů podle odstavce 1 a o blokování, opravě, doplnění nebo likvidaci osobních údajů. To neplatí, pokud je informování příjemce nemožné nebo by vyžadovalo neúměrné úsilí.

**~~Práva subjektu údajů ve vztahu ke správci a zpracovateli~~** ~~(~~[~~nařízení EU č. 2016/679, 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) (populární název "GDPR" z anglického General Data Protection Regulation)~~](http://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016R0679&from=en)~~) - Od května(máj) 2018 nabude účinnosti~~

**GDPR novinka - Pověřenec pro ochranu osobních údajů (DPO - Data Protection Officer)**

* Povinnost pověřence:
  + zpracování provádí orgán veřejné moci či veřejný subjekt, s výjimkou soudů jednajících v rámci svých soudních pravomocí
  + 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
  + hlavní činnosti správce nebo zpracovatele spočívají v rozsáhlém zpracování zvláštních kategorií údajů
  + V dalších případech pokud to uvede zákon
* Může být víc správců na jednoho pověřence

**GDPR novinka – Posouzení vlivu zpracování**

<https://www.systemonline.cz/it-security/posouzeni-vlivu-na-ochranu-osobnich-udaju-dle-gdpr.htm>

* “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 “
  + Tato definice zjednodušeně říká, že pokud se organizace rozhodne zpracovávat osobní údaje, měla by posoudit, jakým způsobem toto zpracování může zasáhnout do svobod a práv lidí, tedy jak může ovlivnit jejich životy.
* Posouzení je povinné pri:
  + Profilování a vyhodnocovanie osobných aspektov fyzickej osoby
  + Rozsáhlé zpracování citlivých osobních údajů
  + Rozsáhlé monitorování veřejně přístupných prostor

**Práva subjektu údajů (GDPR)**

* Právo na prístup k osobným údajom
* Právo na opravu osobných údajov
* Právo na vymazanie (zabudnutie)
* Právo na obmedzenie spracovania
* Právo na prenos osobných údajov (ďalšiemu prevádzkovateľovi napr. pri zmene mobil. poskytovateľa)
* Právo namietať spracuvávanie na účely priemého marketing a profilovania

**Teritoriální působnost**

-Článek 4 odst. 1 písm. a) směrnice 95/46 stanoví:

* Každý členský stát použije na zpracování osobních údajů vnitrostátní ustanovení, která přijme na základě této směrnice, pokud:
  + zpracování je prováděno v rámci činností provozovny správce na území členského státu; pokud je stejný správce usazen na území několika členských států, musí přijmout opatření nezbytná pro dodržování povinností stanovených použitelným vnitrostátním právem každou ze svých provozoven“.

- Rozhodnutí SDEU ve věci Google Spain a Weltimmo

-Provozovna = bankovní účet, webová prezentace a stálé právní zastoupení

**GDPR – přeshraniční působnost**

Již aktuální případ – Rozhodnutí Google Spain a CNIL

* Čl. 3 odst. 2 -toto nařízení se vztahuje na zpracování osobních údajů subjektů údajů, které se nacházejí v Unii, správcem nebo zpracovatelem, který není usazen v Unii, pokud činnosti zpracování souvisejí:

1. s nabídkou zboží nebo služeb těmto subjektům údajů v Unii, bez ohledu na to, zda je od subjektů údajů požadována platba
2. s monitorováním jejich chování, pokud k němu dochází v rámci Unie.

* Problémy:
  + Vymáhání práva
  + „Všechno nebo nic“

**9) Informace veřejného sektoru – pojem, česká a evropská právní úprava**

Pojem *informace veřejného sektoru*

Za informace veřejného sektoru (anglicky „Public Sector Information“ – dále v textu i PSI) jsou (podle Evropské směrnice 2003/98/EC) považovány veškeré **dokumenty**, **databáze** a **další** **informace**, které sbírá, uchovává a zpracovává veřejný sektor. Jsou chápány jako tzv. „dynamické znalosti“, které neustále proudí, proměňují se v čase, mají určitou časově omezenou platnost. Např. informace o **počasí**, o **dopravní** **situaci**, o aktuální **vlastnické struktuře** **obchodní společnosti**, o **platných zákonech** apod.

Obsah veřejného sektoru (anglicky „Public Sector Content“ – PSC) představuje **shromážděné**, **zpracované**, **utříděné** a **uložené** **informace**, které mají charakter spíše „statických znalostí“. Jsou to např. muzejní sbírky, vzdělávací programy, umělecká díla, knihy, obrazy, vědecké práce, výsledky výzkumu apod.

Oba pojmy se v některých dokumentech označují společným termínem „Informace/obsah veřejného sektoru“, anglicky Public Sector Information/Content, zkratka PSI/C.

Evropské směrnice 2003/98/EC byla do našeho právního řádu zavedena formou několika drobných ustanovení, kterými byl novelizován zákon o svobodném přístupu k informacím.

<https://ikaros.cz/vyzkum-informaci-verejneho-sektoru-ceske-republiky>

**Obsah** – zejména digitální – je vynikajícím zdrojem pro následné využití komerční i nekomerční sférou a přináší možnosti vzniku služeb s přidanou hodnotou.

Příkladů okolo nás vidíme celou řadu:

* **Úkolem veřejného sektoru** – např. obchodních soudů – je v souladu se zákonem registrovat firmy a vést o nich zákonem předepsané záznamy v podobě obchodního rejstříku. Zákon ukládá tuto „listinu“ – dnes tedy již vlastně databázi - zveřejnit. Tyto základní záznamy o firmách mohou posloužit jako zdroj pro další informační služby, např. pro poskytování hospodářských či kreditních informací, ekonomické analýzy, ratingové služby apod.
* **Úkolem hydrometeorologického** **ústavu** financovaného z veřejných zdrojů je monitorovat počasí a vydávat předpovědi. Meteorologická data však mohou posloužit také komerčním subjektům, např. pojišťovnám při ověřování pojistných událostí, mobilním operátorům, pro vytvoření služby s přidanou hodnotou, které poskytuje předpověď počasí podle místa pobytu účastníka sítě.
* **Úkolem zeměměřičského ústavu či katastrálního úřadu** je evidovat a zpracovávat informace o území. Tyto informace – zejména jsou-li v digitální podobě - mohou posloužit jako vstupní informace pro komerční mapové služby využívané např. internetovými portály, mobilními operátory, ale také pojišťovnami a síťovými odvětvími.

**Typy informací veřejného sektoru**

Za informace veřejného sektoru jsou podle Evropské směrnice považovány veškeré dokumenty, databáze a další informace, které sbírá, uchovává a zpracovává veřejný sektor. Projekt MEPSIR, který se zabýval výzkumem stavu informací veřejného sektoru v členských státech EU a kterého se účastnila za ČR i EPMA, rozdělil PSI do 6 tématických oblastí:

* Hospodářské informace
* Geografické informace
* Právní informace
* Meteorologické informace
* Sociální informace
* Dopravní informace

Vymezení těchto 6 oblastí ale nepokrývá celé spektrum informací veřejného sektoru. Zcela jistě bychom k nim mohli přiřadit ještě informace **vědecké**, **výzkumné**, **kulturní**, dále informace **produkované** **systémem** **školství** a **zdravotnictví** a **další**. Takto šířeji chápe informace veřejného sektoru OECD (Organizácia pre hospodársku spoluprácu a rozvoj). Evropská komise podporuje aktivity směřující k širšímu využívání informací veřejného sektoru a k vytváření informačních služeb s přidanou hodnotou.

**10) Otevřená data – pojem a právní úprava**

Otevřená data jsou informace a čísla bezplatně a volně dostupná na internetu ve strukturované a strojově čitelné podobě a jsou zpřístupněna způsobem, který jejich využití neklade zbytečné technické či jiné překážky.

Formát a struktura otevřených dat tedy umožňuje jejich hromadné počítačové zpracování, k němuž jejich vydavatel poskytl právní svolení. Díky tomu mohou být dál volně zpracovávány, a to i v rámci softwarových aplikací.

Jedná se například o **jízdní řády**, **příjmy států**, **seznam** **poskytovatelů** **sociálních** **služeb**, kalendář ministra nebo **měření čistoty ovzduší**. Pocházejí z univerzit, nevládních organizací, soukromých firem nebo veřejné správy.

V České republice můžeme díky zákonu o svobodném přístupu k informacím zatím získávat jen část z údajů, které úřady shromažďují. Pokud si o to zažádají a úřad jim vyhoví. Otevřená data by měl naopak zveřejnit sám vydavatel na internetu tak, aby je všichni mohli snadno najít a stáhnout. Otevřená data lze chápat i v širším smyslu - kromě informací veřejné správy lze využít i data komerčních subjektů.

[[*http://www.jaknainternet.cz/page/1701/otevrena-data*](http://www.jaknainternet.cz/page/1701/otevrena-data)](http://www.jaknainternet.cz/page/1701/otevrena-data/)

**Které datasety tedy budou do roka povinně dostupné jako otevřená data?(2016)**

*~~Třináct databází vyjmenovaných v původním návrhu vládního nařízení se v průběhu meziresortního řízení scvrklo na osm. Zhruba do podzimu příštího roku by se měly zveřejňovat zcela volně (prakticky všechna data, která databáze obsahuje, pokud jsou veřejně přístupná), jsou velmi různorodé. Vedle evidencí méně zajímavých pro širší veřejnost, jako je přehled volných služebních míst ve státní správě anebo registr práv a povinností, evidující různá oprávnění veřejných úřadů, však mezi nimi najdeme především celostátní informační systém o jízdních řádech. Definitivně tak skončí podivně a s korupčním nádechem vzniklý monopol na tato data, který si na ministerstvu dopravy před mnoha lety vylobovala jedna brněnská firma.~~*

*~~Dále zde najdeme veřejný rejstřík právnických a fyzických osob (snad i včetně obchodního a živnostenského rejstříku), dotace, veřejné zakázky a registr smluv. Všichni, kteří se těmito databázemi chtějí pracovat „ve velkém“, tak budou mít on-line přístup ke kompletním zdrojovým datům.~~*

*Můžeme jen litovat, že se do přehledu (snad jen zatím) nedostaly některé další zajímavé datasety, jako jsou například aktuální informace o dopravě, vytvářené Centrem dopravního výzkumu, veřejnou výzkumnou institucí v působnosti Ministerstva dopravy, anebo Českým hydrometeorologickým ústavem, příspěvkovou organizací Ministerstva životního prostředí. Jejich zařazení by mohlo překonat dosavadní stav, kdy tyto instituce svá data buď odmítají vůbec poskytovat (viz nominace v soutěži* [*Otevřeno x Zavřeno 2016*](http://oz.otevrenaspolecnost.cz/)*), anebo je poskytují za finančních požadavků, překračujících limity podle Infozákona a směrnice 2003/98/ES o opakovaném použití informací veřejného sektoru (ve znění směrnice 2013/37/EU). V tomto směru stojí před vládou úkol neskončit jen u osmi dosud vybraných databází, ale zařazovat mezi ně další.*

**Obecná právní úprava otevřených dat**

**Zákon č.** [**106/1999 Sb**](https://www.zakonyprolidi.cz/cs/1999-106)**., o svobodném přístupu k informacím**

-OD = Kvalifikovaný způsob poskytování informací zveřejněním

* OD Novela zákona č. [298/2016 Sb.](https://www.zakonyprolidi.cz/cs/2016-298) (Účinnost od 1. 1. 2017)
* Navazuje na PSI novelu – z. č. [222/2015 Sb.](https://www.zakonyprolidi.cz/cs/2015-222) (Účinnost od 10.09.2015 )

**§ 3 odst. 11:***„Otevřenými daty se pro účely tohoto zákona rozumí informace zveřejňované způsobem umožňujícím dálkový přístup v otevřeném a strojově čitelném formátu, jejichž způsob ani účel následného využití není omezen a které jsou evidovány v národním katalogu otevřených dat."*

**Pro připomenutí - § 3 odst. 7 a 8:**

* Strojově čitelným formátem se pro účely tohoto zákona rozumí formát datového souboru s takovou strukturou, která umožňuje programovému vybavení snadno nalézt, rozpoznat a získat z tohoto datového souboru konkrétní informace, včetně jednotlivých údajů a jejich vnitřní struktury.
* Otevřeným formátem se pro účely tohoto zákona rozumí formát datového souboru, který není závislý na konkrétním technickém a programovém vybavení a je zpřístupněn veřejnosti bez jakéhokoli omezení, které by znemožňovalo využití informací obsažených v datovém souboru.

**Právní úprava OD v ČR – nová povinnost publikovat**

* **§ 4b odst. 2:***„Povinné subjekty zveřejňují informace obsažené v jimi vedených nebo spravovaných registrech, evidencích, seznamech nebo rejstřících, které jsou na základě zákona každému přístupné a které lze využít při podnikání nebo jiné výdělečné činnosti, ke studijním nebo vědeckým účelům anebo při veřejné kontrole povinných subjektů, jako otevřená data. Povinné subjekty zaevidují tyto informace v národním katalogu otevřených dat. Seznam informací podle věty první stanoví prováděcí právní předpis."*
* Zmocnění Vlády vydat nařízení, kterým určí informace povinně poskytované jako OD („povinné datové sady“) = nastartování ekosystému OD.

**Návrh nařízení vlády – „Povinná otevřená data“**

* účinnost 1. 1. 2018
* Údaje ze systému ARES *(Účelem www aplikace ARES Ministerstva financí je zpřístupnit údaje z informačních systémů pro vedení registrů a evidencí veřejné správy o ekonomických subjektech.)*
* Rejstříky (Obchodní, Spolkový)
* Jízdní řády
* Metadata registru smluv
* Evidence obsazovaných míst
* Údaje z informačního systému o veřejných zakázkách
* Dotace
* Držitelé datových schránek