

Nařízení EP a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (GDPR) – *executive summary*

Dovolte, abychom Vás stručně seznámili se základními pravidly, která s účinností nařízení EU (GDPR) upraví nakládání s osobními údaji:

Nařízení EP a Rady (EU) 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů (*General Data Protection Regulation*)

Je závazné? od 25. 5. 2018 bezprostředně použitelné (28 členských států + státy EFTA, aplikační přednost, ponechává však národním státům pravomoci k jeho provedení a úpravě, zvláště v oblasti citlivých osobních údajů, připouští *lex specialis* (zákony proti praní špinavých peněz)

Koho zavazuje? - každého, kdo zpracovává data fyzických osob

správce = fyzickou nebo právnickou osobu, orgán veřejné moci, agentura nebo jiný subjekt, který sám nebo společně s jinými určuje účely a prostředky zpracování osobních údajů (i správce mimo EU, pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb - musí jmenovat zástupce, který nese odpovědnost)

zpracovatele = fyzickou nebo právnickou osobu, orgán veřejné moci, agentura nebo jiný subjekt, který zpracovává osobní údaje pro správce

jaké výjimky má malý podnik do 250 zaměstnanců? nemusí každé zpracování osobních údajů evidovat, ledaže zpracování, které provádí, pravděpodobně představuje riziko pro práva a svobody subjektů údajů, zpracování není příležitostné, nebo zahrnuje zpracování zvláštních kategorií údajů, nemusí určit pověřence DPO

Co se chrání?

všechny osobní údaje = veškeré informace o identifikované nebo identifikovatelné fyzické osobě (fyzická osoba, kterou lze přímo či nepřímo identifikovat, zejména odkazem na určitý identifikátor, například jméno, identifikační číslo, lokační údaje, síťový identifikátor nebo na jeden či více zvláštních prvků fyzické, fyziologické, genetické, psychické, ekonomické, kulturní nebo společenské identity)

- bez ohledu na jejich státní příslušnost nebo bydliště, nevztahuje se na osobní údaje právnických osob
- nevztahuje se na zpracování osobních údajů fyzickou osobou v rámci činnosti čistě osobní povahy nebo činnosti prováděné výhradně v domácnosti (ale hostingové služby pro činnosti osobní povahy ano)
- souhlas nutný i pro uchovávání cookies¹ nebo jiné identifikátory
- zvláštní podmínky pro zpracování osobních údajů, které vypovídají o rasovém či etnickém původu, politických názorech, náboženském vyznání či filozofickém přesvědčení nebo členství v odborech, a zpracování genetických údajů, biometrických údajů za účelem jedinečné identifikace fyzické osoby a údajů o zdravotním stavu či o sexuálním životě nebo sexuální orientaci fyzické osoby

¹ **Cookies** = současná právní úprava se právní úprava řídí § 89 odst. 3 ZoEK, ohledně něhož se vedou spory, zda je založen na principu opt-in nebo opt-out; GDPR výslovně uvádí síťový identifikátor jako možný osobní údaj s tím, že výjimkou z povinnosti získat souhlas subjektu údajů je mimo jiné zpracování oprávněných zájmů správce, přičemž ta za takový oprávněný zájem je výslovně uznán i přímý marketing (na ten se však samozřejmě vztahuje princip opt-out).

Pro posuzování „oprávněného zájmu“ však bude klíčové „rozumné očekávání“ subjektů údajů (jaký účel, dobu, rozsah atd. mohl očekávat)

I do působnosti GDPR je rozumné vykládat českou úpravu za opt-in

dopadá na **každé zpracování** = jakoukoliv operaci nebo soubor operací s osobními údaji nebo soubory osobních údajů, který je prováděn pomocí či bez pomoci automatizovaných postupů, jako je shromáždění, zaznamenání, uspořádání, strukturování, uložení, přizpůsobení nebo pozměnění, pseudonymizace², vyhledání, nahlédnutí, použití, zpřístupnění přenosem, šíření nebo jakékoliv jiné zpřístupnění, seřazení či zkombinování, omezení, výmaz nebo zničení

- technologicky neutrální, aplikuje se jak při automatizovaném, tak manuálním zpracování (údajů evidovaných nebo takových, které mají být do evidence vloženy)
- osobní údaje subjektů údajů nacházejících se v Unii uskutečněné správcem nebo zpracovatelem, jenž není v Unii usazen, pokud činnosti zpracování souvisejí s nabídkou zboží nebo služeb těmto subjektům údajů bez ohledu na to, zda je spojena s platbou

Nutné kroky:

1. zmapovat, kde všude jsou osobní údaje uloženy
2. zjistit, kdo má právo s nimi manipulovat
3. odhalit, kdo všechno k nim má přístup a proč
4. vyřešit šedou zónu IT, kdy jsou data uložena mimo k tomu určená úložiště (neoficiální zálohy, data v telefonech zaměstnanců, apod.)

Co hrozí za porušení?

Pokuta až 20.000.000 euro nebo 4 % z celkového ročního obrátu společnosti (vyšší z obou možností) v závislosti na faktorech, jako jsou např. povaha, závažnost a délka porušování, počet poškozených občanů a míra škody, kroky podniknuté správcem či zpracovatelem ke zmírnění škod, kategorie osobních údajů dotčené porušením a řada dalších.

Vedle pokuty hrozí žaloby fyzických osob na náhradu hmotné i nehmotné újmy.

Co je pro zpracování povinné? splnit jednu z těchto podmínek a pouze v odpovídajícím rozsahu:

- subjekt údajů udělil souhlas se zpracováním svých osobních údajů pro jeden či více konkrétních účelů
- nezbytné pro splnění smlouvy, jejíž smluvní stranou je subjekt údajů, nebo pro provedení opatření přijatých před uzavřením smlouvy na žádost tohoto subjektu údajů
- nezbytné pro splnění právní povinnosti, která se na správce vztahuje
- nezbytné pro ochranu životně důležitých zájmů subjektu údajů nebo jiné fyzické osoby
- nezbytné pro splnění úkolu prováděného ve veřejném zájmu nebo při výkonu veřejné moci, kterým je pověřen správce;
- 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

² „pseudonymizace“ - zpracování osobních údajů tak, že již nemohou být přiřazeny konkrétnímu subjektu údajů bez použití dodatečných informací, pokud jsou tyto dodatečné informace uchovávány odděleně a vztahují se na ně technická a organizační opatření, aby bylo zajištěno, že nebudou přiřazeny identifikované či identifikovatelné fyzické osobě

Jaká práva má subjekt zpracování?

- na přístup ke svým osobním údajům
- být informován o vhodných zárukách
- na kopii osobních údajů, přenositelnost
- na opravu nepřesných nebo neúplných údajů
- na výmaz („právo být zapomenut“) nebo na omezení zpracování

Jaké odpovídající povinnosti z toho vyplývají správci?:

1. umožnit subjektu přístup k osobním údajům:

- o účelu zpracování
- o kategorii dotčených osobních údajů
- o příjemci nebo kategorii příjemců, kterým osobní údaje byly nebo budou zpřístupněny, zejména příjemci ve třetích zemích nebo v mezinárodních organizacích
- o plánované době, po kterou budou osobní údaje uloženy, nebo kritéria použitá ke stanovení této doby
- o zdroji osobních údajů
- o skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování³

2. informovat subjekt o vhodných zárukách

3. opravit nepřesné nebo neúplné údaje

4. poskytnout kopie osobních údajů

5. umožnit přenositelnost (portabilitu) = fyzická osoba má právo na kopii zpracovaných osobních údajů o ní v podobě, která umožňuje přenést zpracované údaje k jinému poskytovateli služby

- jen data získaná od subjektu a týkající se subjektu (široký výklad, tj. i poskytnutá jen udělením práv aplikaci; co údaje o protistraně? ta nový zpracovatel nesmí zpracovávat)
- např. nakoupené položky, playlist, kontakty z emailu (neukládá-li zpracovatel, nemusí předat)
- o tomto právu musí zpracovatel subjekt informovat

³ zákaz **automatizovaného individuálního rozhodování, včetně profilování** - právo nebýt předmětem žádného rozhodnutí založeného výhradně na automatizovaném zpracování, včetně profilování, které má pro něho právní účinky nebo se ho obdobným způsobem významně dotýká

Výjimky:

- pokud je rozhodnutí nezbytné k uzavření nebo plnění smlouvy mezi subjektem údajů a správcem údajů
- povoleno právem
- založeno na výslovném souhlasu subjektu údajů

„profilování“ = jakákoli forma automatizovaného zpracování osobních údajů spočívající v jejich použití k hodnocení některých osobních aspektů vztahujících se k fyzické osobě, zejména k rozboru nebo odhadu aspektů týkajících se jejího pracovního výkonu, ekonomické situace, zdravotního stavu, osobních preferencí, zájmů, spolehlivosti, chování, místa, kde se nachází, nebo pohybu;

▪

- jak rychle? bezodkladně (= do měsíce)
- bezplatně
- forma: strojově čitelné (= zachovat informace vč. metadat, tj. ne PDF)

6. **vymazat** („právo být zapomenut“; RTBF) nebo **omezit zpracování**, pokud:

- osobní údaje již nejsou potřebné pro účely, pro které byly shromážděny nebo jinak zpracovány
- subjekt údajů odvolá souhlas, na jehož základě byly údaje zpracovány
- subjekt údajů vznese námitky proti zpracování
- osobní údaje byly zpracovány protiprávně
- osobní údaje musí být vymazány ke splnění právní povinnosti
- osobní údaje byly shromážděny v souvislosti s nabídkou služeb informační společnosti

Jak tedy správce musí postupovat? musí sám posoudit vliv na ochranu osobních údajů s cílem posoudit konkrétní pravděpodobnost a závažnost vysokého rizika a zohlednit přitom povahu, rozsah, kontext a účely zpracování a zdroje rizika

Co z toho pro správce vyplývá?

1. **získat souhlas** = jednoznačné potvrzení - vyjádřením svobodného, konkrétního, informovaného a jednoznačného svolení subjektu údajů ke zpracování osobních údajů

jak? prokazatelně, nejlépe písemné prohlášení (i elektronicky) nebo ústní, mlčení souhlasem není

souhlas dítěte až od 16 let (národní státy mohou snížit až na 13)

Souhlas není svobodný, pokud subjekt údajů nemá skutečnou nebo svobodnou volbu nebo nemůže souhlas odmítnout nebo odvolat, aniž by byl poškozen. Souhlas není platný, je-li mezi správcem a subjektem jasná nerovnováha

Zpracování osobních údajů pro jiné účely, než jsou ty, pro které byly osobní údaje původně shromážděny, by mělo být povoleno pouze v případě, kdy je slučitelné s účely, pro které byly osobní údaje původně shromážděny

Správce nesmí pátrat po dalších údajích, které by mu FO umožnily identifikovat

Odvolat souhlas musí být stejně snadné jako jej poskytnout

2. **postupovat transparentně** = subjekt musí dostat stručné, snadno přístupné a srozumitelné informace, podávané za použití jasných a jednoduchých jazykových prostředků, v elektronické podobě na webu, o:

- právu na přístup ke shromážděným osobním údajům, které se ho týkají (strukturované, strojově čitelné)
- právu na opravu osobních údajů, které se jí týkají
- „právu být zapomenut“

Subjekt údajů by měl mít právo nebýt předmětem žádného rozhodnutí, a to včetně opatření, které hodnotí osobní aspekty týkající se jeho osoby, vychází výlučně z automatizovaného zpracování a které má pro něj právní účinky nebo se jej podobně významně dotýká, jako jsou automatizované zamítnutí on-line žádosti o úvěr nebo postupy elektronického náboru bez jakéhokoliv lidského zásahu

3. **přijímat námitky** = jsou-li osobní údaje zpracovávány pro účely přímého marketingu, měl by mít subjekt údajů právo kdykoli bezplatně vznést námitku proti tomuto zpracování, včetně profilování, v rozsahu, v němž souvisí s daným přímým marketingem, ať již jde o počáteční, nebo další zpracování – na to musí být subjekt zřetelně a výslovně upozorněn

4. **přijmout opatření (kodex)** a informovat subjekt bezplatně o:

- totožnosti a kontaktních údajích správce a jeho případného zástupce a případného pověřence pro ochranu osobních údajů
- účelu zpracování, pro které jsou osobní údaje určeny, a právním základu pro zpracování
- případných příjemcích nebo kategorie příjemců osobních údajů
- úmyslu správce předat osobní údaje do třetí země nebo mezinárodní organizaci a existenci či neexistenci rozhodnutí Komise o odpovídající ochraně
- době, po kterou budou osobní údaje uloženy, nebo není-li ji možné určit, kritériích použitá pro stanovení této doby
- právu požadovat od správce přístup k osobním údajům týkajícím se subjektu údajů, jejich opravu nebo výmaz, popřípadě omezení zpracování, a vznést námitku proti zpracování, jakož i práva na přenositelnost údajů
- právu odvolat kdykoli souhlas, aniž je tím dotčena zákonnost zpracování založená na souhlasu uděleném před jeho odvoláním
- právu podat stížnost u dozorového úřadu
- skutečnosti, zda poskytování osobních údajů je zákonným či smluvním požadavkem, nebo požadavkem, který je nutné uvést do smlouvy, a zda má subjekt údajů povinnost osobní údaje poskytnout, a ohledně možných důsledků neposkytnutí těchto údajů
- skutečnosti, že dochází k automatizovanému rozhodování, včetně profilování

5. **jmenovat DPO – Data Protection Officer** (inspektora, pověřence) ochrany údajů

víc než Compliance nebo ISO 9001 – také IT procesy, technologie

explicitně stanovena pro orgány veřejné moci, správce nebo zpracovatele, jejichž hlavní činnost spočívá v operacích, které kvůli své povaze, rozsahu a/nebo účelu vyžadují pravidelné a systematické monitorování subjektů údajů v širokém rozsahu anebo jejichž hlavní činnosti spočívají ve zpracování zvláštních kategorií osobních údajů. V jiných případech to bude určovat národní zákon

6. vést záznamy o zpracování osobních údajů

7. ohlašovat případy narušení bezpečnosti = jednat bez odkladu a je-li to možné, ohlásit dozorovému úřadu a subjektu (popsat povahu porušení, doporučení subjektu); kdy nemusí ohlašovat? jestliže:

- správce zavedl náležitá technická a organizační ochranná opatření a tato opatření byla použita u osobních údajů dotčených porušením zabezpečení osobních údajů, zejména taková, která činí tyto údaje nesrozumitelnými pro kohokoli, kdo není oprávněn k nim mít přístup, jako je například šifrování, nebo
- správce přijal následná opatření, která zajistí, že vysoké riziko pro práva a svobody subjektů údajů podle odstavce 1 se již pravděpodobně neprojeví, nebo
- vyžadovalo by to nepřiměřené úsilí. V takovém případě musí být subjekty údajů informovány stejně účinným způsobem pomocí veřejného oznámení nebo podobného opatření.

8. provádět posouzení dopadu na ochranu osobních údajů = systematický popis zamýšleného zpracování, posouzení rizik z hlediska práv a svobod subjektů údajů, provedení testu proporcionality včetně posouzení, zda je zpracování ve vztahu k deklarovaným účelům nezbytné. Vypracování takového posouzení by mohlo být delegováno na inspektora pro ochranu údajů, pokud bude danou společností jmenován

- kdy? při zpracování citlivých údajů, systematického monitorování veřejně přístupných míst nebo systematického a rozsáhlého vyhodnocování osobních aspektů fyzických osob, včetně profilování
- posuzovat přiměřenost zásahu do práv druhých, jejichž údaje budou předmětem zpracování, ještě před zahájením samotného zpracování, v současnosti vyplývá pro správce z obecných principů ochrany osobních údajů obsažených ve směrnici, zejména z povinnosti správce stanovit legální a legitimní účel zpracování, zpracovávat osobní údaje pouze na základě řádného právního titulu a v přiměřeném rozsahu

9. předběžné konzultace = vyplýve-li z posouzení, že zpracování bude vysoce rizikové a riziko nelze zmírnit přiměřenými prostředky, pokud jde o dostupnost technologií a nákladů na jejich zavedení – pokud se nenajdou žádná dostupná opatření, zpracování lze provést

10. Jestliže osobní údaje nebyly získány od subjektu údajů, poskytne správce subjektu údajů informace o:

- zdroji, odkud správce osobní údaje získal
- totožnosti a kontaktních údajích správce a případně jeho zástupce, případného pověřence pro ochranu osobních údajů
- účelu zpracování, pro které jsou osobní údaje určeny, a právním základem pro zpracování
- kategorii dotčených osobních údajů
- případném příjemci nebo kategorii příjemců osobních údajů
- případném záměru správce předat osobní údaje příjemci ve třetí zemi

Věříme, že pro Vás uvedené informace jsou užitečné, a jsme připraveni Vám se splněním požadavků GDPR pomoci

za #svlaw
Petr Horáček
tel. 602 742 675
petr@horacek.eu

o autorovi:

Mgr. Petr Horáček, LL.M., advokát

Absolvent Právnické fakulty Univerzity Karlovy v Praze (Mgr., 2001), Nottingham Trent University (LL.M., 2012)

- od roku 2001 se jako právník zabývá moderními technologiemi (mj. vedení pracovní skupiny Ministerstva vnitra ČR a APVTS pro záznam a odposlech telekomunikačního provozu)
- finanční ředitel a investor (Infinity a.s.), výkonný ředitel (MULTIMA a.s.) IT firem
- samostatný advokát (obchodní právo, veřejné zakázky, korporátní právo - fúze, akvizice, přeshraniční struktury, MBO...)
- publikační a přednášková činnost. Anglický a německý jazyk

Specializuje se na:

- obchodní právo
- trestní právo
- občanské právo
- veřejné zakázky
- fúze a akvizice
- GDPR, eIDAS
- MBO

