SEDLAKOVA
LEGAL

# Hlídač právních předpisů
# Červenec 2020

## Co jsme si pro Vás v červnenci připravili?




+420 733 555 958 gdpr@sedlakovalegal.com www.sedlakovalegal.com Purkyňova 648/125, 612 00 Brno, Czech Republic | 28. října 2566/124, 702 00 Ostrava

## Novinky

### Systémy externích dodavatelů a odpovědnost správce

Mnozí určitě znají situaci, kdy zakoupí do společnosti systém, který vytvořil externí dodavatel. Může se jednat například o docházkový systém. Docházkový systém však umožňuje ukládání nadbytečných osobních údajů, či má nastaveny delší doby výmazu, než je ze zákona vyžadováno. Úřad pro ochranu osobních údajů (**Úřad**) upozorňuje, že v případě, že bude zahájena u společnosti kontrola, nemůže společnost argumentovat, že příslušný informační systém je dodáván externím dodavatelem a některé funkcionality vyplývají z nastavení tohoto systému. Je totiž primární povinností správce, tedy společnosti, která si docházkový systém od dodavatele zakoupila, dodržovat všechny zásady a povinnosti vyplývající z GDPR.

Úřad též upozorňuje, že nelze automaticky předpokládat splnění všech povinností ochrany osobních údajů pouze na základě skutečnosti, že je stejný informační systém využíván taktéž dalšími obdobnými správci.

### Jak správně provádět videokonference

Národní úřad pro kybernetickou a informační bezpečnost a Národní agentura pro komunikační a informační technologie vytvořili bezpečnostní standard pro videokonference. Dokument je dostupný zde: https://www.govcert.cz/download/kii-vis/obecne/2020-07-17_Standard-pro-VTC_1.0.pdf

Doporučujeme, aby s tímto dokumentem byly seznámeny osoby odpovědné za správu IT systémů ve společnosti. V dokumentu je totiž prakticky vysvětleno, jaké řešení pro videokonference vybrat a bezpečnostní doporučení a požadavky, kterými je potřeba se řídit.

## Zrušení možnosti předávat osobní údaje do USA – co teď?

Dne 16. 7. 2020 vydal Soudní dvůr Evropské unie (**SDEU**) rozhodnutí známé jako Schrems II. Předmětem rozhodnutí bylo zejména zrušení tzv. Privacy shield a možnost využívání Standardních smluvních doložek v podobě, ve které byly využívány doposud. Než však vysvětlíme, v čem je rozhodnutí přelomové, je potřeba si zjednodušeně připomenout, jak probíhá předávání do třetích zemí.

### Kdy mohu předávat osobní údaje?

EU vytvořila přijetím GPDR pomyslnou ochranou zeď, která obklopuje její vnější hranice. Pokud bude chtít kterákoliv společnost z EU předat osobní údaje do státu, který se nachází za její zdí, bude muset zajistit, že v dané zemi bude odpovídající úroveň ochrany předaných osobních údajů. Způsobů, kterými tak lze učinit je více:

1. Třetí země je na seznamu zemí, které představují odpovídající ochranu

Tato první možnost závisí na aktivitě Evropské komise. Ta může rozhodnout, že některé země mají nastavenou ochranu osobních údajů, jako státy v EU. Pokud dojde k vydání takového rozhodnutí, je možno do této země předávat osobní údaje, jako by se jednalo o stát EU (seznam všech takových zemí zde https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en). Příkladem je například Nový Zéland, Israel, Faerské ostrovy, Argentina, Švýcarsko, Israel, Japonsko, či také USA. Předání do USA bylo limitováno pouze na společnosti, které jsou registrovány pod tzv. Privacy shield. To znamená, že společnost v USA musela projít složitým registračním procesem, ve kterém se zavázala, že bude dodržovat velké množství povinností vztahujících se k ochraně osobních údajů. Pokud třetí země není na seznamu zemí, které představují odpovídající ochranu, je potřeba zajistit jiný způsob předání.

2. Jiným způsobem může být zajištění vhodných záruk

Tyto další způsoby již závisí pouze na aktivitě správců a zpracovatelů osobních údajů. Patří mezi ně například uzavření standardních smluvních doložek, či přijetí závazných podnikových pravidel. Právě jedním z nejčastějších způsobů je uzavření standardních smluvních doložek. Evropská komise vydala vzorové standardní smluvní doložky, které je potřeba doslovně převzít, vyplnit a uzavřít s druhou stranou. Existuje několik verzí těchto doložek, přičemž vždy záleží, zda budou mimo EU předávány osobní údaje správci, nebo zpracovateli. Standardní smluvní doložky jsou zveřejněny zde: https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.

3. Alternativy pro specifické situace

GDPR pamatuje také na některé specifické situace. Do třetí země lze předat osobní údaje dle čl. 49 GDPR také se souhlasem subjektů údajů, který byl řádné informován o rizicích. Popřípadě je předání nutné pro splnění smlouvy mezi subjektem údajů a správcem, z důvodu veřejného zájmu apod. Typický příklad je možnost předání osobních údajů zaměstnance ve chvíli, kdy mu zaměstnavatel zařizuje ubytování či letenky pro pracovní cestu v cizině. Tato alternativa by však neměla být využívána pro pravidelná a opakovaná předávání, pro ty je potřeba využít například některý ze způsobu uvedený v bodě 2.

## Kdy mohu předat osobní údaje do země mimo EU/EHP?

**Stát byl zařezen do seznamu zemí s odpovídající ochranou (např. Israel, Švýcarsko)**

Pokud není na seznamu zemí

**Se společností musím uzavřít standardní smluvní doložky, či musím mít schválená závazná podniková pravidla, nebo schválené kodexy chování (stále však musím kontrolovat, jaké má země předpisy na ochranu osobních údajů)**

**NEBO**

**Bude k předávání docházet na základě výjimky dle čl. 49 GDPR, tedy například informuji subjekty o rizicích a získám jejich souhlas, či je předání nezbytné pro splnění smlouvy atp.**

### Co se rozhodnutím Schrems II stalo?

SDEU rozhodnutím zrušil Privacy shield, tedy automatickou možnost předávat osobní údaje bez dalšího společnostem v USA, které jsou pod Privacy shield registrovány. V rozhodnutí nebyla stanovena ani žádná „ochranná doba“, tudíž byl Privacy shield zrušen hned k 16. 7. 2020. V rozhodnutí SDEU rovněž konstatoval, že pokud bude předávání prováděno na základě standardních smluvních doložek, musí správce před předáním osobních údajů zhodnotit, zda daná třetí země nepředstavuje pro osobní údaje riziko (zda například daný stát má k datům přístup a může je zneužít atp.). Nepostačí tedy jen „slepě“ uzavřít standardní smluvní doložky, ale bude potřeba zhodnotit, jak jsou v daném státě řešeny předpisy na ochranu osobních údajů.

> *Zajímavost:* V rozhodnutí SDEU uvedl, že USA je velmi nebezpečnou zemí, neboť bezpečnostní složky v USA mohou mít přístup k datům z EU a obyvatelé EU se u amerických soudů proti tomuto nemohou bránit.

### Co to pro Vás může znamenat?

Pokud využíváte například cloudové úložiště americké společnosti (AWS, OneDrive) či služeb některých jiných amerických společnosti, jako například Mailchimp, DigitalOcean, Google, může být takové předávání v současné chvíli nelegální. Tyto společnosti byly registrovány právě pod Privacy shield. Jeho zrušením je však potřeba hledat jiný způsob, jakým budou data předávána.

Co teď?

V EU se rozjely dva názorové proudy. Dozorové úřady některých států (Německo) okamžitě vydaly stanoviska, že je potřeba okamžitě zastavit jakékoliv předávání do USA a přenést data zpět do EU. Jiné úřady (Anglický, Francouzský, Španělský) se vyjádřily zdrženlivě a vyzvaly správce, ať prozatím vyčkávají, dokud nevydají stanovisko, jak dále pokračovat. Český Úřad pro ochranu osobních údajů se k tomuto vyjádřil dne 7. 8. 2020 na svých webových stránkách: https://www.uoou.cz/uoou-k-nbsp-dopadum-zruseni-stitu-soukromi-eu-usa-na-spravce/d-43874

Z tohoto důvodu navrhujeme následující praktický postup:

1. Zkontrolujte uzavřenou zpracovatelskou smlouvu se společností z USA (často nazvána jako Data Processing Addendum) zda obsahuje všechna ustanovení a přílohy standardních smluvních doložek.

    a) Pokud standardní smluvní doložky neobsahuje – kontaktujte tuto společnost s žádostí o jejich uzavření, popřípadě jí je předložte vyplněné k podepsání.

2. Aktualizujte své zásady ochrany osobních údajů v oblasti příjemců osobních údajů, kde je potřeba uvést, na základě jakých vhodných záruk jsou osobní údaje předávány konkrétním příjemcům (tedy i společnostem v USA). Zároveň je vhodné do zásad uvést, jak jsou jejich osobní údaje chráněny a jaká rizika plynou z předání.

3. Dle Úřadu je potřeba s každým v USA, komu předáváte osobní údaje uzavřít standardní smluvní doložky a řešit s ním konkrétní dopady rozsudku. Rovněž by bylo dle Úřadu nejvhodnější zajistit další bezpečnostní záruky (např. uložení dat včetně metadat pouze na území EU, šifrování bez zadních vrátek apod.).

Nezapomínejte, že smlouvu uzavíráte se společnosti z USA, která nemusí být přesně znalá evropského práva. Proto je potřeba věnovat zvýšenou pozornost přesnosti standardních smluvních doložek. Jakákoliv změna textace by totiž měla za následek to, že by se už nejednalo o standardní smluvní doložky. Tím by tedy nebyla naplněna odůvodněnost předávání do třetí země a takové pozměněné doložky by musel schválit dozorový úřad.

Rovněž nás neváhejte kontaktovat na adrese gdpr@sedlakovalegal.com, pokud si nebudete vědět rady, či budete chtít poradit.

## Recept na správně nastavené cookies na webu

V minulém měsíci jsme požádali Úřad o zpřístupnění všech protokolů z kontrol věnujících se souborům cookies. Jednotlivé protokoly jsou dostupné zde:

https://www.uoou.cz/poskytnuta%2Dinformace%2Ddne%2D10%2Dcervence%2D2020/ds-6313/archiv=0&p1=2567.

Protokol z kontroly může sloužit jako velmi dobrý pomocník, neboť se v něm Úřad podrobně zabývátím , co požadoval předložit, jak hodnotil nastavení procesů a jaký je jeho názor na danou věc. Rovněž je však potřeba upozornit, že se jedná pouze o názory jednotlivých kontrolorů, které se mohou v případném správním řízení, či v jiných případech lišit.

Už v minulém hlídači jsme psali o tom, že český zákon o elektronických komunikacích, který řeší právě oblast cookies, byl špatně novelizován a umožňuje využívání tzv. OPT-OUT možnosti. Pro připomenutí tedy uvádíme několik bodů, které ukazují, jak lze v českém prostředí využívat soubory cookies:

- Není potřeba získávat aktivní souhlas, dle metodiky Úřadu se za aktivní souhlas považuje přednastavený prohlížeč, který ukládání cookies umožňuje. V cookie liště tedy postačí uvést obdobné věty: *„Nastavením Vašeho prohlížeče takovým způsobem, který umožňuje ukládání souborů cookies souhlasíte s jejich ukládáním. Můžete se však rozhodnout cookies blokovat.“* Následně by měl existovat proklik na více informací, kde se uživatel dozví další podrobné údaje o souborech cookies.
- Vždy je potřeba uživatele řádné informovat dle čl. 13 a 14 GDPR, a to například prostřednictvím cookie lišty. Způsob ukládání cookies může být také například součástí Privacy policy. Je však potřeba, aby byl dokument jednoduše dostupný. Jedno z porušení, které Úřad shledal, bylo například to, že Privacy policy nebyly na úvodní stránce, ale pod záložkou kontakty, což musel uživatel těžce hledat.

Co si nachystat pro případnou kontrolu:

- Zásady používání souborů cookies
- Interní dokumentaci, jenž obsahuje způsoby nakládání s osobními údaji uvnitř společnosti (směrnice o ochraně soukromí, směrnice o zásadách bezpečnosti, směrnice o nakládání se soubory cookies atp.)
- Zpracovatelské dodatky či zpracovatelské smlouvy se společnostmi, které Vám zajišťují služby spojené se soubory cookies
- Záznamy o činnostech zpracování
- Analýzu rizik spojená se zpracováním souborů cookies – včetně tzv. balančního testu

Zásady používání souborů cookies

V zásadách by měly být uvedeny jednotlivé cookies (_ga, _gat…), účel jejich použití, doba uložení a nejlépe také právní titul, na základě kterého jsou využívány. Rovněž musí být v cookies policy uvedeno, jakých služeb třetích stran je využíváno (Google, Facebook atp.),

včetně odkazu na jejich zásady užívání cookies. Rovněž by měla být obsažena informace o právech subjektů údajů. Vzorové cookie policy, ze kterých je možno vycházet, jsou například v tomto kontrolním protokolu (Zásady jsou uvedeny na straně 18-21): https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=43387.

Interní dokumentace

Tuto dokumentaci si nechává Úřad předložit z toho důvodu, aby vyhodnotil, jak máte uvnitř společnosti řešeny procesy nakládání s osobními údaji. Nejvhodnější je přímo v interní dokumentaci stanovit způsob nastavování cookies na webu, analýzy rizik, DPIA apod.

Zpracovatelské a další dodatky

Pokud Vám s nastavením cookies na webu pomáhají externí dodavatelé, nezapomeňte na zpracovatelské dodatky s těmito dodavateli. Obdobně, pokud využíváte služeb třetích stran, jako například Google Analytics, zkontrolujte podmínky, které jste při nasazení na webu odsouhlasili. Součástí by měla být ustanovení o zpracování osobních údajů. Pokud například máte na webových stránkách tlačítko „Like" od společnosti Facebook, jste společně s Facebookem tzv. společnými správci, což by měla opět reflektovat příslušná dohoda.

Záznamy o činnostech zpracování

Je potřeba evidovat, jaké činnosti zpracování jsou prováděny. Kromě záznamů je vhodné také vést seznamy, jaké konkrétní cookies jsou užívány. Příkladem může být předložený dokument v jedné z kontrol:

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| contento_ratings | tzv.first party cookie | zajištění bezp. přecházení podvodům a odstraňování chyb | funkční cookies | session (relace) | identifiíkace v rámci hlasování-cookie zamezuje opětovnému hlasování (např. v anketách) | oprávněný zájem | ne |
| anka + (ID) | tzv. first party cookie | zajištění bezp. předcházen podvodům a ostraňování chyb | funkční cookies | session (relace) | identifikace v rámci hlasování-cookie zamezuje opětovnému hlasování (např. v anketách | oprávněný zájem | ne ne |
| quiz + (ID) | tzv. first party cookie | zajištění bezp. předcházení podvodům a odstraňování chyb | funkční cookies | session (relace) | identifikace v rámci hlásování – cookie zamezuje opětovnému hlasování (např. v anketách) | oprávněný zájem | ne |
| gtm_userStatus i[redacted] | tzv.first party cookie | vývoj a zlepšování produktů | analytické a výkonnostní soubory cookies | session (relace) | identifikace stavu návštěvníků-přihlášen/ nepřihlášen. Hodnota cookies slouží pro analytické přehledy využívání produktu, případně A/B testování- tedy modifikace obsahu pro přihlášené/nepřihlášené návštěvníky | oprávněný zájem | ne |
| PHPSESSID | tzv. first party cookie | vytvoření pro- filu pro personalizovaný obsah | funkční cookies | session (relace) | toto je všeobecný identi- fikátor používaný na udržování proměnných uživatele. Zpravidla se jedná náhodně vygenerované číslo | oprávněný zájem | ne |

Analýza rizik

Kromě všech výše uvedených dokumentů by každý správce měl mít řádně zdokumentovaná rizika, která se pojí s ukládáním cookies. Rozsah analýzy rizik se bude lišit dle účelů cookies (rozsáhlá analýza bude muset být provedena například u marketingových cookies, kde dochází k personalizaci chování uživatelů atp.). Součástí analýzy by mělo být vyhodnocení, jaká újma může subjektům hrozit v různých situacích a jaké zranitelnosti zpracování představuje. Pokud je zpracování založeno na oprávněném zájmu, měl by součástí analýzy rizik být tzv. balanční test, ve kterém bude zhodnoceno, zda zájem správce převažuje zájem subjektu údajů.

## Jak kontrola probíhá?

Kontrola probíhá velmi jednoduše. Úřad si nechá vyžádat veškerou výše uvedenou dokumentaci, může si rovněž požádat o print screeny různých částí webů, interních součástí atp. Následně může požádat o vysvětlení některých cookies, účelů, zabezpečení atp. Úřad následně bude při kontrole hodnotit, zda jsou splněny základní zásady dle GDPR, zda je plněna informační povinnost dle čl. 13 a 14 GDPR, zda máte uzavřené příslušné smlouvy, zajišťujete bezpečnost, vedete záznamy o činnostech zpracování apod.

Nutno podotknout, že dokumentace, která je potřebná, je opravdu rozsáhlá. Z tohoto důvodu je potřeba doporučit, abyste přípravu nepodceňovali. Ač existují lhůty, do kterých musíte dokumenty Úřadu předložit, nejsou natolik dlouhé, abyste stihli veškerou dokumentaci připravit „na poslední chvíli".

## Závěr

Červenec byl na novinky v oblasti ochrany osobních údajů velmi bohatý. Bohužel přinesl hodně problémů mnohým správcům, kteří využívají služeb společností z USA. Pevně věříme, že v měsíci srpnu se dozvíme podrobnější instrukce, jak předávat osobní údaje do USA, popřípadě jaké procesy pro takové předávání nastavit.