SEDLAKOVA LEGAL

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.com

SOUBORY COOKIES – METODICKÝ POKYN

Tento dokument slouží jako návod, jak pracovat se soubory cookies z právního pohledu. V dokumentu jsou komplexně řešeny povinnosti, které je potřeba v souvislosti s nastavením cookies na webu splnit. Tento dokument slouží pouze jako obecný popis povinností a postupů při zavádění cookies na webu.

CO TO JSOU SOUBORY COOKIES A JAK JE ROZLIŠOVAT?

Soubory cookies jsou malé textové soubory, které se ukládají do prohlížeče a slouží k mnoha účelům, jako například analýzám, marketingu, správnému fungování webu, nastavení jazyka webu atp. Úprava ukládání cookies je zakotvena primárně v § 89 odst. 3 zákona o elektronických komunikacích. Toto ustanovení stanovuje, že každý, kdo ukládá cookies je povinen předem uživatele prokazatelně informovat o rozsahu a účelu jejich zpracování a je povinen nabídnout jim možnost takové zpracování odmítnout.

Tato povinnost neplatí pro technické ukládání nebo přístup výhradně pro potřeby přenosu zprávy prostřednictvím sítě elektronických komunikací nebo je-li to nezbytné pro potřeby poskytování služby informační společnosti, která je výslovně vyžádána účastníkem nebo uživatelem.

Z legálního hlediska je proto potřeba cookies rozdělit na dvě oblasti:

1. Technické (nezbytné) cookies – takové cookies, které jsou potřebné pro správné zobrazení stránky. Typicky se bude jednat o následující druhy cookies:

a) **„User-input“ cookies** – slouží k tomu, aby si zapamatovali určitý input uživatele na webu, jako například uložení informací vyplněných ve formuláři, který má více stránek nebo nákupní košík.

b) **Autentizační cookies** – kontrolují, zda se uživatel již například přihlásil do svého uživatelského účtu.

c) **Bezpečnostní cookies** – takové, které kontrolují bezpečné užívání stránek, nadměrné žádosti uživatelů (neúspěšné pokusy o přihlášení) atp.

d) **Multimediální cookies (flash cookies)** – takové, které ukládají technická data potřebná k tomu, aby byl přehrán video či audio obsah.

e) **UI cookies** – cookies umožňující nastavení jazyka, počet zobrazených produktů na stránce atp.

2. Další cookies – ostatní cookies, které slouží k marketingu, analýzám, trackování uživatelů na webu, nahrávání a zkoumání jejich aktivity, profilování atp.

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.com

Pro technické cookies tak platí, že je možné je ukládat a není potřeba vyžadovat souhlas s jejich uložením, neboť se předpokládá, že jsou potřebné pro chod webu. **Stále je však potřeba o všech cookies uživatele informovat (podrobněji níže).**

Dle zákona o elektronických komunikacích platí, že je možno zpracovávat soubory cookies tehdy, kdy je uživatelům nabídnuta možnost zpracování odmítnout. Tento režim znamená, že soubory cookies je možno ukládat do té doby, než uživatel „zaklikne", že s ukládáním nesouhlasí (této možnosti se říká OPT-OUT). Takto nastavený model je v Evropě unikátní, neboť Česká republika špatně implementovala směrnici, ze které tato úprava vychází. V okolních státech je tak potřeba pro ukládání cookies (netechnických) žádat aktivní souhlas (OPT-IN). Až po získání tohoto souhlasu je možné cookies ukládat.

Český Úřad pro ochranu osobních údajů prováděl v tomto roce několik kontrol a dospěl k závěru, že je potřeba držet se **znění českého zákona o elektronických komunikacích, a tedy je možno využívat režim OPT-OUT.** Je však potřeba upozornit, že může dojít k novelizaci zákona, či přijetí tzv. ePrivacy nařízení. V takovém případě s nejvyšší pravděpodobností přejde i Česká republika na povinný režim OPT-IN.

KDY ZVOLIT OPT-OUT A KDY OPT-IN A JAK?

OPT-OUT je vhodné volit tehdy, kdy budou ukládány pouze základní analytické cookies, například prostřednictvím Google Analytics. V ostatních případech, kdy bude patrné, že může být zasaženo do soukromí uživatelů výraznějším způsobem, doporučujeme volit OPT-IN možnost.

OPT-IN doporučujeme volit vždy v následujících případech:

- Využívání cookies, které nahrávají aktivitu uživatelů (pro analytické účely) – například využívání HotJar.
- Marketingové cookies – jakékoliv cookies, které budou sloužit k tomu, aby byly o uživatelích sbírána data, která následně budou využívána k remarketingu, personalizované nabídce zboží, včetně marketingových plug-inů pro sociální sítě.
- Jakékoliv další cookies, u kterých bude vyhodnoceno, že by je uživatel na webu nemusel očekávat.

Jak získat souhlas s ukládáním cookies?

Souhlas musí splňovat náležitosti stanovené v GDPR, tedy musí být **aktivní, svobodný, informovaný a jednoznačný.**

Aktivní – uživatel musí aktivně odsouhlasit ukládání cookies (zakliknout check-box). Nepostačí aktivita, jako například „scrollování" stránkou dolů atp.

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.com

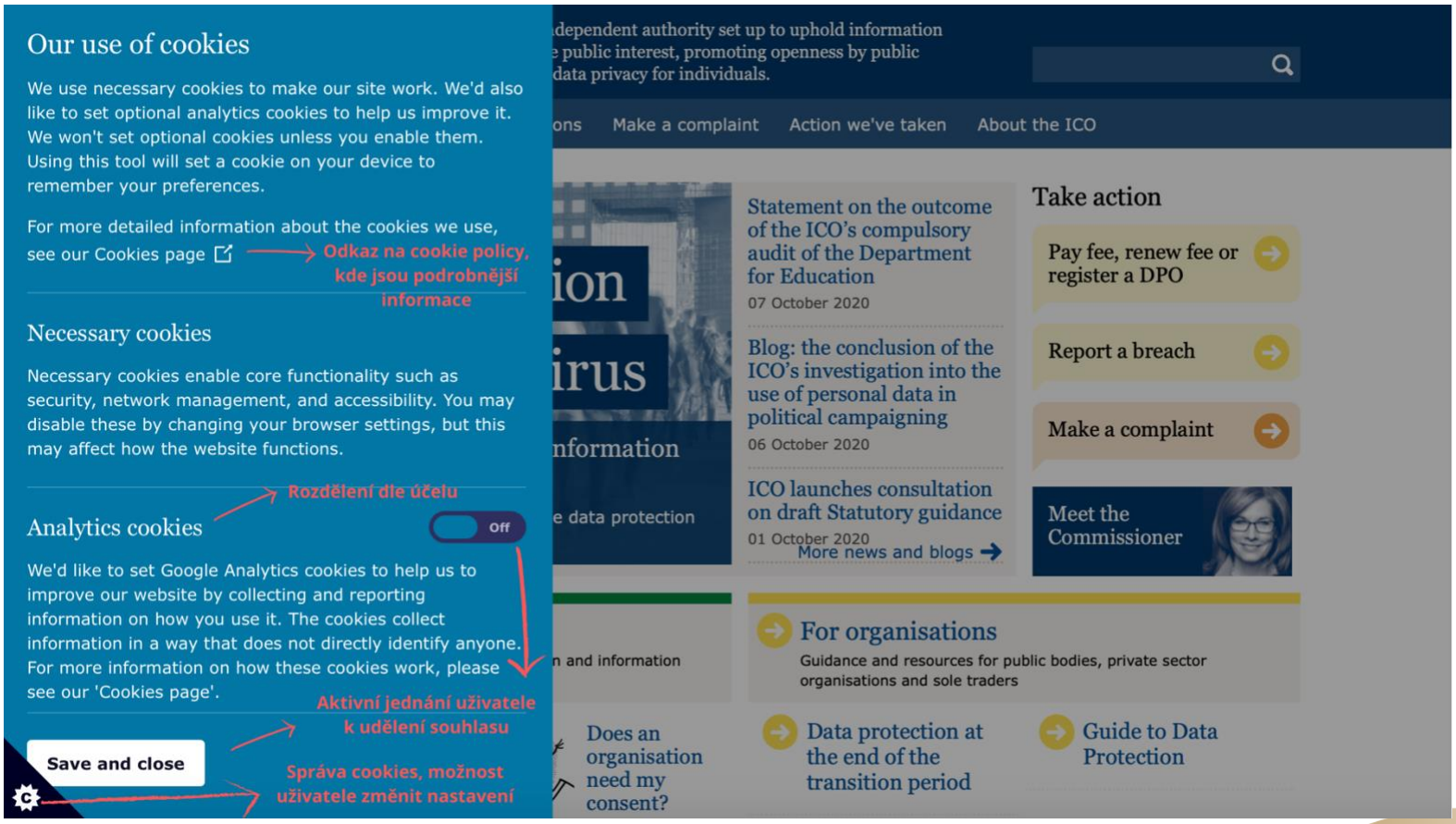
Svobodný – uživatel nesmí být nucen k udělení souhlasu. Z tohoto důvodu jsou zakázány tzv. cookie walls. Není možné zobrazit uživateli cookie lištu přes celou obrazovku, která nejde skrýt a uživatel si tak nemůže prohlížet obsah webu.

Informovaný – uživatel musí vědět, pro jaké účely souhlas uděluje, dostane dostatečné informace o tom, kdo cookies zajišťuje, jak dlouho jsou uchovány atp.

Jednoznačný – pro různé účely musí být souhlas zvlášť. Pokud tak například budete využívat marketingové cookies a zároveň nahrávat obrazovku uživatele pro analýzy, je potřeba tyto dva účely rozdělit na dva samostatné souhlasy. Uživatel si přitom může vybrat, se kterými soubory cookies souhlasí a se kterými nikoliv. Není potřeba získávat pro každý jednotlivý soubor cookie souhlas zvlášť, lze je generalizovat do různých skupin. V rámci podrobnějších informací však musí být uvedeno, co se pod jednotlivými skupinami nachází za konkrétní soubory cookies.

Uživatel by měl mít vždy také možnost své preference změnit, tzn. někde na webové stránce by měl mít přístup ke správě souborů cookies.

Příkladem, jak by ideálně mělo vypadat získání souhlasu s ukládáním cookies, je webová stránka Britského úřadu pro ochranu osobních údajů (ICO: https://ico.org.uk + ve VB platí obecná povinnost OPT-IN):



+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.com

Jak pracovat s OPT-OUT možností?

U opt-out možnosti je dostatečné zobrazit uživateli např. cookie lištu, či na webových stránkách **viditelně** umístit informaci o ukládání cookies, přičemž součástí toho je potřeba uvést, že používáním webové stránky bude docházet k ukládání cookies a opět dát uživatelům možnost takové ukládání odmítnout (ve správě cookies, případně dle názoru Úřadu pro ochranu osobních údajů postačí, když informujete uživatele, že existují nástroje, jak ukládání souborů cookies blokovat).

Shrnutí

V ČR lze prozatím využívat OPT-OUT možnost, tedy ukládat soubory cookies do té doby, než je uživatel odmítne. Tuto možnost však doporučujeme pouze ve chvíli, kdy bude na webu prováděna základní analytika. V ostatních případech doporučujeme OPT-IN s náležitostmi uvedenými výše. U technických cookies není potřeba získávat souhlas. O všech cookies však musí být uživatel informován.

CO UVÉST V INFORMACÍCH O UKLÁDÁNÍ COOKIES?

Jak je uvedeno výše, odkaz na využívání cookies musí být jednoduše dostupný. Informace o cookies se nesmí skrývat pod dalšími odkazy. Nejvhodnější je uvést odkaz na cookies přímo na úvodní stránce, v cookie liště atp.

V zásadách by měly být uvedeny následující informace:

- Vysvětlení, co jsou to soubory cookies;
- Jednotlivé cookies (technické cookies, _ga, _gat, marketingové cookies…);
- Účel jejich použití (nejlépe pro každý soubor cookies zvlášť);
- Doba uložení (session, 1 hodina, 7 dní, 2 měsíce…) a nejlépe také právní titul, na základě kterého jsou využívány (souhlas, oprávněný zájem);
- Jakých služeb třetích stran je využíváno (Google Analytics, Facebook Pixel, HotJar atp.), včetně odkazu na jejich zásady užívání cookies;
- Informace o právech subjektů údajů;
- Pokud budete využívat pro vyhodnocování souborů cookies externí subjekty (marketingové agentury), informace o tomto předání.

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. V těchto cookie policy nejsou uvedeny jednotlivé druhy cookies (toto však doporučujeme, z důvodu aktuální judikatury SDEU). Nedoporučujeme rovněž kopírovat tyto cookie policy, nýbrž využít je pouze jako možný způsob textace.

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.com

INTERNÍ DOKUMENTACE

Interní pokyny o zabezpečení a práce s osobními údaji

U správce by měl existovat interní dokument, který komplexně řeší nakládání s osobními údaji a práci se soubory cookies. Měl by primárně řešit způsob ukládání, práci s cookies, vyřizování práv subjektů údajů a další bezpečnostní a procesní pravidla, která se budou lišit dle rozsahu využívaných cookies. U jednoduchých analytických cookies postačí základní definování, kdo bude mít k souborům přístup, jak je řešena otázka odmítnutí/souhlasu, co dělat, když dojde k úniku získaných dat atp.

Posouzení vlivu na ochranu osobních údajů

U rozsáhlejších marketingových cookies, kde dochází k personalizaci a určitému profilování uživatelů, bude potřeba vyhodnotit, zda je potřeba zpracovat tzv. posouzení vlivu na ochranu osobních údajů dle čl. 35 GDPR (obecně známe jako DPIA). Metodu vyhodnocení potřebnosti DPIA uvádí Úřad pro ochranu osobních údajů na svých webových stránkách: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38940. Samotné provádění DPIA poté popsal v (prozatím) navrženém metodickém pokynu: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=38693. Povinnost provádět DPIA se však bude zejména vztahovat k rozsáhlým profilováním uživatelů, kteří navíc mohou být určitým způsobem zranitelní. Tuto povinnost není potřeba plnit ve chvíli, kdy nebudou cookies obsahovat žádné osobní údaje.

Záznamy o činnostech zpracování (seznamy užívaných cookies)

Pokud soubory cookies ukládají osobní údaje (informace, pomocí kterých jste schopni identifikovata konkrétní osobu), je potřeba evidovat záznamy o činnostech zpracování. Ty by měly obsahovat náležitosti dle čl. 32 odst. 1 GDPR. Jak mohou záznamy vypadat, uvádí ÚOOÚ na svých webových stránkách: https://www.uoou.cz/assets/File.ashx?id_org=200144&id_dokumenty=30188.

Rovněž je vhodné uchovávat přehled o všech cookies, které jsou využívány. V rámci záznamu může být uvedeno jaké druhy cookies jsou na webových stránkách zpracovávány, k čemu slouží, o jaký druh cookies se jedná, jak dlouho jsou uchovány, co daná cookie dělá a právní titul. Příkladem může být předložený dokument v jednom protokolu z kontroly:

název	*typ*	*účel*	*vlastník*	*doba trvání*
IMRID	třetí strany persistentní	měření sledovanosti videa společností Nielsen, možnost optout v nastavení uživ. profilu	Nielsen	13 měsíců
SSCVER	třetí strany persistentní	měření sledovanosti videa společností Nielsen, možnost optout v nastavení uživ. Profilu	Nielsen	13 měsíců
_ga	třetí strany persistentní	statistika a vyhodnocování účelu návštěvy Google Analytics	Google	2 roky

+420 733 555 958
office@sedlakovalegal.com
www.sedlakovalegal.com

Zpracovatelské a další dodatky

Pokud Vám s nastavením cookies na webu pomáhají externí dodavatelé, nezapomeňte na zpracovatelské smlouvy či 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 (opět by tato dohoda měla být součástí odsouhlasených podmínek).

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.

V případě, že budou využívány pouze základní analytické cookies, které neukládají osobní údaje (Google Analytics v základní podobě), domníváme se, že taková analýza není nezbytně nutná. Úřad pro ochranu osobních údajů by si ji však mohl vyžádat.

CO SI NACHYSTAT?

- 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

Závěr

Oblast cookies je velmi rozsáhlá, přičemž vždy bude také záležet na konkrétním balíčku cookies užívaný na webových stránkách. Doporučujeme vždy nasazení cookies konzultovat s odborníkem.

Tento metodický pokyn byl vyhotoven ke dni 7. 10. 2020.