

Doporučení k zpracování *cookies* a obdobných prostředků sledování od 25. května 2018

- (1) Toto doporučení je vydáno s přihlédnutím k častým dotazům ze strany veřejnosti, po projednání s ministerstvem průmyslu a obchodu a s přihlédnutím k článku 57 odst. 1 obecného nařízení o ochraně osobních údajů.¹ Do dokumentu byly zapracovány připomínky z veřejné diskuse k návrhu doporučení.
- (2) Jednou z důležitých otázek ochrany soukromí na internetu je používání *cookies*, počítačových souborů, které mimo jiné umožňují jednoznačně rozpoznat přístroj, a jiných obdobných prostředků používaných k rozlišení koncových zařízení uživatelů (jedná se například o otisky zařízení, angl. *device fingerprinting*).²
- (3) Rozřešení těchto otázek je důležité pro praxi. Ačkoliv *cookies* identifikují toliko koncové zařízení, používá-li ho více uživatelů, je nutno vycházet z toho, že jsou srozuměni s tím, jak je nastaveno, protože jinak by si ho nastavili jinak. Obdobně na pracovišti může nastavit koncové zařízení zaměstnavatel a zaměstnanec je s tím srozuměn, i když by si třeba přál nastavit ukládání *cookies* jinak.

Jak kombinovat GDPR se směrnicí o ePrivacy transponovanou do ZEK?

- (4) Právní regulace *cookies* je v současné době stanovena zákonem č. 127/2005 Sb., o elektronických komunikacích (ZEK), který je transposicí stávající směrnice o *ePrivacy*.³ Nové nařízení o *ePrivacy*⁴ má být speciálním právním předpisem k GDPR. Je zřejmé, že nařízení o *ePrivacy* nebude schváleno ke dni účinnosti GDPR 25. května 2018⁵ a bude tak třeba přihlédnout jak ke stávající sektorové národní regulaci, tak k některým pravidlům pro zpracování osobních údajů podle GDPR, což článek 95 GDPR i výslovně uznává.
- (5) *Cookies* dílčím způsobem upravuje zejména § 89 odst. 1 a 3 ZEK. Toto ustanovení je transposicí článku 5 odst. 3 směrnice o *ePrivacy*, který byl novelizován směrnicí 2009/136/ES⁶ a do českého právního řádu byl transponován zákonem č. 468/2011 Sb.

¹ Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 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), CELEX: 32016R0679, GDPR.

² Stanovisko pracovní skupiny WP-29 číslo WP224

http://collections.internetmemory.org/haeu/20171122154227/http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp224_en.pdf

³ Směrnice Evropského parlamentu a Rady 2002/58/ES ze dne 12. července 2002 o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (Směrnice o soukromí a elektronických komunikacích), CELEX: 32002L0058.

⁴ Rada EU projednává návrh nařízení Rady a Evropského parlamentu o respektování soukromého života a ochraně osobních údajů v elektronických komunikacích a o zrušení směrnice 2002/58/ES (nařízení o soukromí a elektronických komunikacích) (nařízení o *ePrivacy*, CELEX: 52017PC0010), které má nahradit stávající směrnici 2002/58/ES o soukromí a elektronických komunikacích (směrnice o *ePrivacy*).

⁵ Návrh nařízení o *ePrivacy* za ČR nyní vyjednává ministerstvo průmyslu a obchodu.

⁶ Aktuální znění článku 5 odst. 3: „Členské státy zajistí, aby uchovávání informací nebo získávání přístupu k již uchovávaným informacím bylo v koncovém zařízení účastníka nebo uživatele povoleno pouze pod podmínkou, že dotčený účastník či uživatel poskytl svůj souhlas poté, co mu byly poskytnuty jasné a úplné informace v souladu se směrnicí 95/46/ES, mimo jiné o účelu zpracování. To nebrání technickému ukládání nebo takovému přístupu, jehož jediným účelem je provedení přenosu sdělení prostřednictvím sítě elektronických komunikací, nebo je-li to

- (6) Ustanovení § 87 odst. 2 ZEK dává subjektu údajů možnost udělit souhlas také pomocí elektronických prostředků. Jednou z možností udělení souhlasu je tak vyplnění elektronického formuláře na Internetu a další jsou podrobněji popsány níže.

Souhlas prostřednictvím nastavení prohlížeče

- (7) Uživatel určuje v nastavení svého PC, resp. v nastavení prohlížeče, zda má prohlížeč umožnit webovské stránce ukládat *cookies* do koncového zařízení.⁷ Toto nastavení lze považovat za **souhlas** se zpracováním osobních údajů. Prohlížeč je nástrojem zprostředkování souhlasu. Souhlas však nemůže zhojit jiné nedostatky, resp. nezákonnosti zpracování osobních údajů.
- (8) Souhlas splňuje definiční znaky souhlasu podle článku 4 bodu 11 GDPR: Je svobodný, konkrétní, informovaný a jednoznačný. Souhlas je vykládán ve vztahu k účelu, prostředku a způsobu zpracování osobních údajů, nikoliv k produktu či webovské aplikaci, tedy je nadbytečné jednou udělený paušální souhlas například pro *cookies* třetích stran dále konkretizovat pro jednotlivý vyhledávač nebo zpravodajský server.
- (9) Správce i v takovém případě plní informační povinnost, tj. poskytne informaci o tom, v jakém rozsahu a pro jaký účel budou osobní údaje zpracovány, kdo a jakým způsobem bude osobní údaje zpracovávat a komu mohou být osobní údaje přímo zpřístupněny. Užití pouze vyskakujícího okna nebo lišty nelze vždy doporučit, protože obtěžují uživatele. Popisu zpracování osobních údajů, včetně *cookies*, je vhodné věnovat speciální a snadno dostupnou informační podstránku, nejlépe označenou jako *Cookies*. Prostředky informování by měly být vůči uživateli co nejvíce přehlednější, zejména by informace v souladu s WP259 měly být podány vrstevnatě (granulárně).

Druhy cookies a jak s nimi zacházet

- (10) Z hlediska účelu zpracování lze *cookies* rozřadit na různé druhy. Tento dokument se nevztahuje na *cookies*, k jejichž používání není třeba informovaného souhlasu podle článku 5 odst. 3 směrnice o ePrivacy. Toto doporučení se tedy nevyužije zejména pro technické *cookies*, které jsou potřebné pro správné zobrazení stránky apod., tj. neslouží pro jiné zvláštní, např. marketingové účely. Bližší výčet je uveden ve WP194.
- (11) Pravidla pro využívání *cookies* a obdobných prostředků podle stávající směrnice o ePrivacy transponované do ZEK je nutno vykládat v souladu s řadou obecných zásad pro zpracování osobních údajů tedy také v souladu s pravidly ochrany osobních údajů podle GDPR. Zejména se jedná o:

Obecné zásady

- a) Vycházet z konceptu záměrné a standardní ochrany osobních údajů podle článku 25 GDPR.

nezbytně nutné k tomu, aby mohl poskytovatel služeb informační společnosti poskytovat služby, které si účastník nebo uživatel výslovně vyžádal.“

⁷ R 66 i. f. novelizační směrnice 2009/136/ES zní: „Je-li to technicky možné a efektivní, může být v souladu s příslušnými ustanoveními směrnice 95/46/ES souhlas uživatele se zpracováním údajů vyjádřen vhodným nastavením prohlížeče nebo jiné aplikace.“

- b) Dodržovat základní zásady zpracování osobních údajů podle článku 5 GDPR. Je nutno jasně formulovat účel zpracování údajů získaných prostřednictvím *cookies* a odvozeně od toho důvod zpracování *cookies* ve vztahu k subjektu údajů. Zvážit, zda se využije R 49 GDPR. Podle článku 6 odst. 1 GDPR rozhodnout, o jaký právní základ se jedná. Pro údaje získané z *cookies* se využijí zejména písmena a), b) a f).
- c) Poskytovat subjektu údajů možnost odvolat souhlas, a to stejným způsobem, jakým byl udělen.
- d) Vyhodnotit riskantnost zpracování osobních údajů. Příliš rozsáhlá kategorisace subjektů údajů, např. na desítky tisíc segmentů trhu, profilování, např. v rámci velkých sociálních sítí, nebude moci být založeno na oprávněném zájmu a bude pro konkrétní profil vyžadovat souhlas podle článku 6 odst. 1 písm. a) GDPR.

Konkrétní pravidla

- e) Prokazatelně a podrobně informovat subjekty údajů o využívání *cookies* nebo obdobných prostředků, tj. k jaké službě se využití váže. Vodítkem k tomu jsou články 13 a 14 GDPR; dále R 30 GDPR a podpůrně R 26 GDPR a R 70 GDPR. To znamená poskytnout informace o tom, v jakém rozsahu a pro jaký účel budou osobní údaje pomocí *cookies* zpracovány, kdo a jakým způsobem je bude zpracovávat a komu mohou být zpřístupněny, a to bez ohledu na právní základ zpracování těchto *cookies*, tedy včetně technických *cookies*. Podle GDPR bude obvykle nakládání s údaji získanými na základě *cookies* zpracováním osobních údajů. *Cookies* se podle článku 4 odst. 1 GDPR dají podřadit pod pojem „síťový identifikátor“.
- f) Zpracovat posouzení vlivu na ochranu osobních údajů (článek 35 GDPR) v případech, kdy má zpracování osobních údajů za následek vznik vysokého rizika, přičemž se tím míní případy, když jsou *cookies* používány pro systematické a rozsáhlé vyhodnocování osobních aspektů, založeném na automatizovaném zpracování podle článku 35 odst. 3 písm. a) GDPR. Jsou-li *cookies* zpracovány ve velkém rozsahu, mělo by být zpracováno posouzení vlivu. Je třeba posoudit vlastní zájmy správce. V ostatních případech není podle WP 248 DPIA třeba.
- g) Správce umožňující svému smluvnímu partnerovi, který bude obvykle v rozsahu získaných údajů a podle charakteru spolupráce samostatným správcem, společným správcem nebo zpracovatelem, umístit jeho *cookies* na své stránky, u společného správce má uzavřenu dohodu, která bude definovat jejich vztahy, u zpracovatele smlouvu o zpracování osobních údajů podle článku 28 GDPR nebo u samostatného správce dohodu stanovící alespoň povinnost smluvního partnera postupovat v souladu s GDPR a ZEK. Zároveň správce zajistí, aby informace o *cookies* umístěná na jeho stránce obsahovala alespoň odkaz na stránky smluvního partnera, v jejichž rámci plní smluvní partner informační povinnosti.
- h) Zajistit, aby v rámci rozhraní pro sdílení profilů mezi jednotlivými reklamními systémy byly skutečně předávány pouze nezbytně potřebné informace s přihlédnutím k článku 5 GDPR a WP171.

- i) Podle článku 17 GDPR *cookies* mazat v krátké lhůtě, tj. nejpozději do 13 měsíců, která je nyní již průmyslovým standardem;⁸ lhůty se počítají od posledního využití *cookies*.

Shrnutí

- (12) Pro *cookies* nezbytně nutné pro zajištění provozu webových stránek a internetových služeb není nutno získat souhlas uživatele (interpretační vodítka k určení takových *cookies* poskytuje WP194). Pro všechny ostatní *cookies* je nutno získat souhlas, který však lze získat nastavením běžných prohlížečů. Pro zpracování osobních údajů získaných na základě takových *cookies* je nutné zvolit vhodný právní základ zpracování podle článku 6 odst. 1 písm. a), b) nebo f) GDPR. Bude-li právním základem souhlas, kritéria souhlasu a další pravidla pro zpracování získaných dat stanoví GDPR. Souhlas je vykládán ve vztahu k účelu, prostředku a způsobu zpracování osobních údajů, nikoliv k produktu či webovské aplikaci, tedy je nadbytečné jednou udělený paušální souhlas například pro *cookies* třetích stran dále konkretizovat pro jednotlivý vyhledávač nebo zpravodajský server.
- (13) Toto doporučení platí od 25. května 2018 do účinnosti (v terminologii EU: „použitelnosti“, angl. „*applicability*“) nového nařízení o *ePrivacy* nebo do vydání stanoviska EDPB. Pro detaily o stavu vyjednávání budoucí právní úpravy *ePrivacy* je třeba kontaktovat příslušný ústřední správní úřad, ministerstvo průmyslu a obchodu.

Vybraná stanoviska WP-29, která mají význam pro *cookies*

1. WP171: stanovisko č. [2/2010](#) k internetové reklamě zaměřené na chování
 2. WP194: stanovisko č. [4/2012](#) k výjimce z požadavku na souhlas s *cookies*
 3. WP208: pracovní dokument č. [2/2013](#) poskytující doporučení, jak získat souhlas s *cookies*
 4. WP224: stanovisko č. [9/2014](#) k uplatňování směrnice 2002/58/ES na otisky zařízení
 5. WP248: [pokyny k posouzení vlivu na ochranu osobních údajů a ke stanovení, zda zpracování bude „pravděpodobně mít za následek vysoké riziko“ pro účely Nařízení 2016/679](#)
 6. WP259: [vodítka k souhlasu podle Nařízení 2016/679](#)
- (14) Případné připomínky a dotazy pošlete na email: posta@uoou.cz.

⁸ Cf. doporučení CNIL ke *cookies* z 5. prosince 2013. Francouzsky: <https://www.cnil.fr/fr/cookies-traceurs-que-dit-la-loi> a anglicky: <https://www.cnil.fr/en/cookies-cnil-extends-monitoring-beyond-website-publishers>.