SVAZ PRŮMYSLU A DOPRAVY
ČESKÉ REPUBLIKY

POZICE SP ČR K NÁVRHU NAŘÍZENÍ O SOUKROMÍ A ELEKTRONICKÝCH KOMUNIKACÍCH - ePRIVACY

Evropská komise představila dne 10. ledna 2017 návrh nařízení upravující směrnici o zpracování osobních údajů a ochraně soukromí v odvětví elektronických komunikací (tzv. ePrivacy).

Hlavním cílem tohoto návrhu je zrevidovat stávající směrnici k ePrivacy, která byla naposledy aktualizována v roce 2009. Tato směrnice obsahuje specifická pravidla týkající se zpracovávání osobních dat v sektoru elektronických komunikací tak, aby byla poskytnuta jasnější pravidla práv spotřebitelů ve vztahu k soukromí (zejména prostřednictvím požadavků na cookies a zneužití osobních údajů).
Toto nařízení by se mělo vztahovat na poskytovatele služeb elektronických komunikací, na poskytovatele veřejně dostupných seznamů a na poskytovatele softwaru umožňujícího elektronické komunikace včetně získávání a prezentování informací na internetu. Toto nařízení by se rovněž mělo vztahovat na fyzické a právnické osoby, které služby elektronických komunikací používají k zasílání přímých marketingových obchodních sdělení nebo ke shromažďování informací souvisejících s koncovými zařízeními koncových uživatelů nebo uložených v těchto zařízeních.
Toto nařízení by se mělo vztahovat na data elektronických komunikací zpracovávaná v souvislosti s poskytováním a používáním služeb elektronických komunikací v Unii, bez ohledu na to, zda ke zpracování dochází v Unii, či nikoli. Nařízení by se rovněž mělo vztahovat na data elektronických komunikací zpracovávaná v souvislosti s poskytováním služeb elektronických komunikací koncovým uživatelům v Unii ze zemí mimo Unii.

Dle stávajícího návrhu nařízení lze předpokládat zásadní dopad na průmysl, podniky či poskytovatele služeb a také na další rozvoj digitální ekonomiky, inovativních řešení a nových business modelů.

Shrnutí pozice SP ČR

Svaz průmyslu a dopravy ČR (SP ČR) považuje funkční ochranu osobních údajů a zavádění jednotných pravidel pro podnikání, včetně podnikání v rámci digitální ekonomiky napříč celou EU za nezbytnou součást rozvoje digitálního trhu. SP ČR má však k návrhu nařízení několik zásadních výhrad. Tou hlavní výhradou je podoba návrhu, který modernizuje směrnici z roku 2002, avšak nově se přetransformoval do podoby nařízení, které má vstoupit v platnost už v květnu 2018. Z pohledu SP ČR tak není dostatek prostoru pro konzultace s podnikatelskou sférou a provozovateli služeb, na které nařízení dopadne. SP ČR považuje za nezbytné, aby legislativní rámec zůstal vyvážený a umožňoval podnikům při zachování účinné ochrany soukromí (včetně soukromí komunikace) inovovat a rozvíjet nové technologie, výrobky a služby. Legislativní opatření by měla být zaváděna pouze tam, kde jsou identifikována selhání trhu.

Komise nedostatečně vyhodnotila dopady tohoto nařízení a ani domácí Ministerstvo průmyslu a obchodu, na nějž SP ČR neustále tlačí, nezapojuje podnikatele a firmy do debat při vytváření instrukcí na jednání na úrovni EU. Jako další problematická ustanovení návrhu nařízení ePrivacy vnímáme následující:

1) **<u>Časový rámec</u> –** Je nutné poskytnout dostatek času na implementaci konečného znění nařízení. Podniky se připravují na *Nařízení o ochraně osobních údajů (GDPR)* a je proto nezbytné zajistit jim dostatek času, aby dobře porozuměly novým požadavkům ePrivacy a mohly se na dodatečné povinnosti připravit. Kolem konečné podoby nařízení panuje značná nejistota, to podnikům znemožňuje zahájit přípravné práce. Protože původně stanovené datum účinnosti nařízení (stejné jako u GDPR) se jeví jako nereálné, **měla by Komise stanovit realistický časový rámec pro přijetí a adaptaci na nařízení.**

2) **<u>Vztah k GDPR</u> –** Nařízení ePrivacy má doplnit GDPR, na jehož implementaci a dalekosáhlé dopady se nyní firmy připravují. Nicméně návrh k ePrivacy se s GDPR překrývá a v mnohém jde ještě dál. **Vztah mezi těmito nařízeními musí být jasně vymezen tak, aby dotčené subjekty věděly, kdy budou aplikována jaká pravidla**.

3) **<u>Rozsah</u>** – Nařízení se dotkne nových typů komunikačních služeb (tzv „over the top services“, dále jen OTT jakými jsou například Skype, Whatsapp a další), poskytovatelů on-line služeb, internetu věcí a také komunikace mezi stroji (tzv. „machine-to-machine communication“ dále M2M). Díky tomu disproporcionálně rozšíří škálu subjektů a služeb, na které se bude vztahovat. Toto by v praxi znamenalo například nutnost speciálního režimu ochrany osobních údajů v tzv. smart zařízeních a vedlo k nutnosti kompletního redesignu průmyslových výrobků na evropském trhu. Tyto požadavky a s nimi související náklady, by tedy vedly snížení konkurenceschopnosti evropských výrobců.

Recitál 11 zmiňuje také subjekty, které užívají elektronickou komunikaci pouze jako doplňkovou službu. To ve svém důsledku znamená, že nařízení dopadne na všechny online služby a bude se vztahovat na téměř všechny poskytovatele služeb. Tímto přístupem se nedosáhne hlavního cíle nařízení, a sice vytvořit rovné podmínky pro poskytovatele elektronických komunikací. Bude to pouze znamenat obrovskou administrativní zátěž pro poskytovatele, kteří nejsou poskytovateli elektronických komunikací, ale využívají elektronickou komunikaci pouze jako doplněk k primární službě (různé plánovače událostí, editování fotografií, mobilní bankovnictví, atd.).

M2M tak, jak je zahrnuta v článku 4(1)(b) a popsána v recitálu (12) znamená, že se týká zpracování a ukládání elektronického obsahu a metadat mezi stroji. Komunikace M2M ve většině případů nezahrnuje osobní údaje (např. chytré zemědělství nebo inteligentní továrny). V komunikaci M2M jsou často užívány neosobní údaje, které jsou však také předmětem tohoto nařízení. Naplnění požadavků vyplývajících z výše zmíněného článku a recitálu bude znamenat významný zásah do systému, v němž různé subjekty elektronicky komunikují napříč dodavatelskými řetězci mezi podniky. V praxi to bude mít negativní dopad na rozvoj a využití nových technologií např. na technologie internetu věcí (IoT) a Průmyslu 4.0. Vybudování infrastruktury, která by byla potřebná k zajištění automatického právně platného souhlasu mezi stroji, by bylo velmi složité, náklady obrovské a v některých případech technicky jen těžko proveditelné.

Teritoriální oblast působnosti, která je rovněž uvedena v čl. 3 odst. 1 písm. b) a c) ve vztahu ke službám a koncovým zařízením, je také velmi problematická a těžko v praxi proveditelná. Tak, jak je formulována znamená, že jakékoli zařízení využívající službu odkudkoliv na světě, pokud se nachází v

EU, musí splňovat požadavky tohoto návrhu. Některá zařízení a služby, které nikdy nebyly uvedeny na trh s úmyslem být nabízeny v EU (například vybavení, které si přivezou zahraniční turisté) budou přesto muset splňovat požadavky tohoto návrhu.

Recitál (11) a veškeré odkazy na komunikaci jako doplňkovou službu by měly být z návrhu vypuštěny.

Recitál (12) a všechny zmínky o komunikaci M2M by měly být z návrhu vypuštěny. Rozsah by měl být zúžen tak, aby explicitně vylučoval průmyslové a B2B aplikace, tedy ty, které nejsou určeny pro koncového uživatele. Pokud jde o osobní údaje v rámci M2M, ty jsou již předmětem GDPR. Tento překryv právních předpisů by znamenal značnou právní nejistotu

Pokud jde o teritoriální pokrytí čl. 3 odst. 1 písm.b) a c) by měl obsahovat odkaz na uvedení na trh EU.

4) **<u>Zajištění důvěrnosti komunikace</u> –** Vezmeme-li v úvahu praktické dopady na síťové operátory a poskytovatele služeb, kteří spoléhají na připojení třetími stranami, je zapotřebí cílenějšího přístupu k požadavkům na důvěrnost. Článek 10, a zejména související odůvodnění, jsou extrémně preskriptivní a neumožňují podnikům, aby v konkurenčním prostředí nadále nabízely svým uživatelům ta nejlepší řešení pro ochranu soukromí. Místo toho je udáván pouze jeden způsob ochrany, který určuje, jak jsou uživatelům představována nastavení ochrany osobních údajů. To bude znamenat významné zatížení podniků, bez toho, aby byla zajištěna účinnější ochrana soukromí.

Článek 10 by měl za následek prudký nárůst blokování souborů cookie třetích stran. Uživatelé budou muset rozhodnout o nastavení ochrany osobních údajů bezprostředně po stažení softwaru. V této době uživatelé nebudou schopni plně posoudit důsledky volby, kterou dělají, protože ještě nezačali používat služby, pro které jsou tyto technologie vyžadovány. To bude mít vážný dopad na podniky, které se využívají služby třetích stran a jejich technologie. Menší vydavatelé, kteří zadávají řízení své reklamy třetím stranám, což je něco, co musí udělat všichni malí vydavatelé, aby byli schopni profitovat z webových stránek, budou obzvláště zasažení. Tento návrh omezí jejich schopnost konkurovat větším podnikům, které se na služby třetích stran spoléhat nemusejí.

Článek 10 a odpovídající body odůvodnění by měly být vypuštěny a namísto toho by měly být řešeny v rámci GDPR.

5) **<u>Důvěrnost a vymáhání práva</u> –** Právo na důvěrnost komunikace by se nemělo vztahovat pouze na komerční sféru. Ochrana udělená Listinou základních práv je univerzální a měla by být zajištěna také v kontextu vymáhání práva a národní bezpečnosti. Jakýkoli mandát, který od poskytovatelů služeb vyžaduje, aby učinili jakákoli opatření k oslabení bezpečnostních / šifrovacích opatření, by měla být výslovně zakázána. Přestože článek 11 odkazuje na čl. 23 odst. 1 písm. e) GDPR, rozšiřují se současná omezení základních práv a svobod ve vztahu k národní bezpečnosti, obraně, veřejné bezpečnosti a předcházení trestné činnosti, finančním zájmům členských států. Tím si orgány členských států rozšiřují přístup k údajům v oblasti daní, veřejného zdraví nebo záležitostí sociálního zabezpečení bez ochrany, která je jinak garantována zákonem.

Navíc podniky nejsou chráněny před požadavky na implementaci backdoor řešení a oslabení svých technologií, jako je šifrování, což umožní větší zásahy členských států do soukromí elektronických komunikací. V případě poskytovatelů on-line služeb, kteří působí v mnoha členských státech, není v čl. 11 odst. 2 rovněž jasné určení jurisdikce v případě konfliktu mezi povinností orgánů zveřejnit údaje na základě žádosti o podnikání. Nařízení ePrivacy, jehož cílem je zajištění důvěrnosti komunikací, nenabízí žádné záruky proti výše zmíněným tlakům.

Ustanovení čl. 23 odst. 1 písm. a) až d) GDPR by se mělo vztahovat na článek 11 tohoto návrhu. Rozšíření možností členských států omezit základní práva na ochranu soukromí občanů by v praxi mohly vést k přijímání legislativy, která by umožňovala nepřiměřené možností sledování. To sotva splňuje celkové cíle Komise, které mají zajistit větší soukromí uživatelů a podporu důvěrnosti komunikací.

Jakýkoli požadavek, který by vedl k oslabení bezpečnosti, by měl být z návrhu vypuštěn. V čl. 11 odst. 2 je třeba další vyjasnění, pokud jde o jurisdikci. Komise by měla tuto oblast hlouběji konzultovat a vyhodnocovat předtím, než budou v rámci tohoto návrhu přijata konkrétní ustanovení.

6) **<u>Koncová zařízení</u>** **–** Přístup k zařízení je vyžadován pro zajištění jeho ochrany. V praxi to probíhá prostřednictvím aktualizací, které jsou nabízeny nebo někdy vyžadovány na základě přístupu k datům. Některé aktualizace jsou nepovinné a jsou prováděny na základě souhlasu uživatele, který tak působí jako kontrolní prvek. Přesto existují případy, kdy je kvůli existenciální hrozbě na síti nutné chránit zařízení provedením aktualizace bez souhlasu uživatele. Nutnost vyžadovat souhlas by představovala příliš vysoké riziko. Podniky také zajišťují ochranu zabezpečením zařízení, jako jsou počítače, tablety, smartphony a jakýmkoliv jiným inteligentním zařízením, která se připojují k internetu. Bez celostního přístupu k ochraně by uživatelé nejen nenakupovali tyto výrobky, ale celé sítě, v rámci kterých tyto výrobky fungují, by byly ohroženy. Proto je zajištění odpovídající úrovně ochrany bona fide v zájmu všech podniků a uživatelů. Článek 8 však vyžaduje souhlas uživatele jako rozhodující způsob ochrany koncových zařízení. Pokud uživatel nebude držet krok s žádostmi o aktualizace, vyvstane vážné riziko ohrožení celých sítí. Zařízení mohou být napadena hackery, aby posílala falešnou komunikaci ostatním uživatelům, narušení ochrany se tak bude šířit velmi rychle. Kromě toho mohou hackeři dokonce přistupovat k sítím a poškozovat je tím, že neposkytnou svůj vlastní souhlas s aktualizací. Také v rámci GDPR se souhlas nepovažuje za svobodně poskytovaný ve vztahu zaměstnavatele / zaměstnance kvůli možné hierarchii. Jak by zaměstnavatelé přiměli své zaměstnance, aby chránili zařízení používaná na pracovišti, jako jsou například počítače či mobilní telefony? Vyžadování souhlasu jako hlavní zákonné metody zpracování, v tomto případě umožní hackerům provádět složitější kybernetické útoky.

Online inzerenti podporují digitální ekonomiku prostřednictvím zpracování informací o webech nebo aplikacích, které spotřebitel používá. To je nezbytné pro měření dopadu inzerátů v rámci nich využívaných. Článek 8 ve svém současném znění tuto praxi omezí. I když obsahuje výjimku pro "měření publika", vztahuje se pouze na situaci, kdy podnik provádí měření prostřednictvím třetích stran. To činí měření neoprávněným pro většinu firem, protože jsou to jen velké online podniky, které jsou schopny provádět měření bez potřeby využití poskytovatele služeb třetích stran. Výjimka také vylučuje měření

reklamy z její oblasti působnosti. Jedná se o zásadní aktivitu pro vývojáře webových stránek a aplikací, aby mohli mimo jiné inzerenty vhodně účtovat za zobrazování reklam. **Pokud by návrh neumožňoval online inzerentům nabízet své služby jako způsob umožňující financování aplikací nebo webových stránek, byly by fungování digitální ekonomiky, vývoj dalších a zkvalitňování stávajících služeb vážně ohroženy. Ve skutečnosti by to znamenalo výhodnější podmínky pro větší podniky s interními online reklamními službami.**

Článek 8 je tak široce pojatý, že se vztahuje i na neosobní údaje a údaje M2M. To se týká inteligentních průmyslových postupů a procesů. Budou roboti a senzory, které shromažďují data ke své údržbě muset dát souhlas vždy, když přijde tento požadavek? To bude nejen velmi nepraktické, pokud jde o efektivnost, ale také technologicky nemožné. Nechápeme, proč by měla být tak přísně regulována neosobní průmyslová data, často zpracovávaná mezi jednotlivými stroji**.**
Toto pojetí ochrany soukromí bude mít také přímý dopad na občany, kteří chtějí využívat interaktivní zařízení (roboty, multimediální monitory), která jsou připojena k centrálním systémům (wifi, bluetooth), aby zodpověděla jejich otázky nebo využívala interaktivní displeje. To může zahrnovat poskytnutí informací o umístění obchodního domu v komerční oblasti nebo nejlepší trasu k autobusové zastávce. Učinit tyto služby užitečnými vyžaduje schopnosti zpracování a ukládání na koncových zařízeních. To se provádí prostřednictvím zákonných dohod mezi, například, subjektem, který je vlastníkem, a subjektem poskytujícím službu. Jak mohou v této souvislosti koncoví uživatelé dát svůj souhlas, když nemají ke koncovému zařízení žádný vztah?

Zákonné možnosti zpracování v článku 6 nařízení GDPR by měly být promítnuty do článku 8 tohoto návrhu.

Do výjimky pro shromažďování údajů o koncových zařízeních podle čl. 8 odst. 1 by mělo být zahrnuto měření dopadu on-line inzerátů na veřejnost třetími stranami. Výjimka by měla umožnit pokračovat v provádění webových analýz s cílem zhodnotit přínosy hodnocení efektivní reklamy. V současné době není jasné, na které "koncové uživatele" se vztahuje čl. 8 odst. 1. Je nutné sladit s GDPR a odkazovat se namísto toho na "subjekt údajů". Je třeba vyjasnit, kdy jde o osobní obsah a kdy o neosobní metadata. V ustanovení čl. 8 odst. 2 je třeba vyjasnit, co se rozumí pojmem "shromažďování informací", zejména zda zahrnuje informace M2M podobně jako článek 6, pokud jde o data elektronických komunikací.

7) **<u>Vymahatelnost</u> –** Pravomoci v oblasti vymahatelnosti by měly být svěřeny veřejnému orgánu, který je v dané věci nejkompetentnější. Otázky týkající se soukromí by měly být řešeny výlučně vnitrostátními orgány pro ochranu osobních údajů. To zajistí větší konzistentnost a zjednodušení a soulad s GDPR. Podniky se tak budou obracet pouze na jednu instituci.

Článek 18 by měl svěřit vymáhání úřadům na ochranu osobních údajů.

8) **<u>Uchovávání údajů a výmaz</u> –** Některé služby závislé na ukládání dat uživatelů, jako je cloud, webmail nebo streamování hudby, potřebují obsah, aby fungovaly a mohly poskytnout spotřebitelům to, co od nich očekávají. Naproti tomu podnikatelé tento obsah využívají nejen k zabezpečení služby,

ale také k vývoji nových produktů a služeb. V průběhu tohoto procesu jsou zákazníkovi poskytnuty srozumitelné a transparentní informace o tom, jak budou jeho data uložena. Spotřebitel má vždy možnost kontrolovat obsah a požádat o jeho smazání.

Tento návrh omezí služby závislé na ukládání dat uživateli. Článek 7 požaduje, aby zpracování a uchovávání údajů bylo anonymizováno nebo údaje vymazány ihned po obdržení. To bude zaznamenat omezení současných a budoucí personalizovaných služeb, které se již nebudou moci spoléhat na datovou komunikaci, jakmile budou data anonymizována. Dále by to znamenalo, že data o obsahu budou po přijetí smazána. U služeb podobných výše uvedeným, spotřebitele očekávají, že jejich data, jako jsou fotografie, e-maily a písně, budou uchovávány pro jejich opětovné zpřístupnění i poté, co budou elektronicky přeneseny. Požadavek na jejich vymazání zabrání podnikům využít dříve shromážděný obsah a metadata k inovacím a vývoji nových služeb pro spotřebitele.

Článek 7 by měl být vypuštěn. Možnost poskytovatelů i nadále poskytovat služby, které se opírají o ukládání obsahu, musí být i nadále zachována. Jinak nebude možné je nadále nabízet v praxi. Navíc, GDPR zajišťuje uživatelům těchto služeb významná práva, včetně práva na vymazání a námitku, a proto bude zabezpečen i nadále vysoký stupeň ochrany soukromí. Článek 5 GDPR, který se týká zpracování osobních údajů, se bude vztahovat také na elektronickou komunikaci. Záměr Komise je sladit návrh nařízení s GDPR. Článek 7 je však v rozporu s tímto cílem a stanoví anonymizaci a vymazání údajů elektronických komunikací ihned po jejich přijetí.

V čl. 7 odst. 1 je také třeba vyjasnit, která práva je třeba v praxi uplatňovat v případě zaznamenávání, ukládání nebo zpracování údajů, například, zda bude právo přenositelnosti údajů uplatněno jako povinnost u dat elektronických komunikací (metadat a obsahu).

9) **<u>Zpracování údajů a souhlas</u>** **–** Návrh nařízení obecně považuje jakékoli zpracování komunikačních údajů pro jiné než základní účely umožnění přenosu komunikace, za mimořádný akt, který je povolen pouze za velmi omezených okolností, většinou znamenajících, že osoba musí udělit souhlas. Tento přístup mohl mít smysl v době, kdy komunikační služby měly omezené funkce, nicméně v dnešní době to nedává smysl. Dnes lidé často volí komunikační službu kvůli jejím chytrým funkcím, které jsou stále více poháněny umělou inteligencí. Tyto funkce, jako je automatické vytváření událostí v kalendáři, zobrazení obsahu "náhledu" pro sdílené odkazy nebo automatizace úkolů, se spoléhají na zpracování komunikačních dat. Článek 6 návrhu ePrivacy by zakázal jakékoliv zpracování nebo zasahování do komunikačních údajů bez souhlasu s úzce vymezenými výjimkami, které by mohly být realisticky použity pouze v omezeném počtu případů, například v oblasti bezpečnosti (čl. 6 odst. 1 písm. Je "nezbytné k udržení nebo obnovení bezpečnosti sítí a služeb elektronických komunikací).“ Tento uzavřený seznam je velmi omezený a není dostatečně pružný, aby byl schopen reagovat na budoucí technologický vývoj. Kromě toho typ souhlasu, který je vyžadován pro zpracování obsahu, jde daleko nad rámec GDPR. Vyžaduje další záruky nad požadavky GDPR: důkaz, že anonymizace byla vyzkoušena a že nefunguje, posouzení dopadů ochrany údajů a předchozí konzultace s Úřadem pro ochranu údajů (UOOU). Ustanovení čl. 9 odst. 3 dále požaduje, aby uživatelé byli žádáni o ověření souhlasu "v pravidelných 6 měsíčních intervalech". Tato kontrola dvakrát ročně je náročná a přísnější než GDPR. Nucení uživatelů, aby každých 6 měsíců znovu potvrzovali svůj souhlas, bude zatěžující pro podniky, obtěžující pro spotřebitele a způsobí, že

spotřebitelé budou ignorovat informace o tom, jak jsou jejich údaje používány v praxi, nemluvě o přidané frustraci vůči zkušenostem se službou. V praxi používá jeden spotřebitel celou řadu aplikací a služeb a tato řada bude i nadále růst.

Článek 6 odst. 2 rovněž rozšiřuje režim souhlasu na metadata. Rozšíření souhlasu s metadaty je pro mnohostranné služby nepraktické - musel by být souhlas vyžadován samostatně? Kromě toho, jak může být shromážděn souhlas od všech stran zahrnutých do automatizované komunikace? To jsou jen některé z důvodů, proč se domníváme, že požadovaný druh souhlasu přesahuje rámec GDPR a může být považován za "souhlas +".
Právní důvody uvedené v článku 6 nařízení o GDPR by měly být zcela promítnuty do článku 6 návrhu o ePrivacy.

Čl. 6 odst. 2 písm. a) a c) by měl být vypuštěn spolu se všemi ostatními odkazy na metadata.

Ustanovení čl. 6 odst. 4 GDPR by mělo v plném znění promítnuto do článku 6 tohoto návrhu, aby bylo povoleno další zákonné zpracování

Slovo "pouze" by mělo být z čl. 6 odst. 3 odstraněno, aby se zlepšila právní jistota návrhu. Jinak se zdá, že čl. 6 odst. 3 je v přímém rozporu s čl. 6 odst. 1. Také se domníváme, že slova "všichni dotčení koncoví uživatelé" by měla být v čl. 6 odst. 3 písm. b) nahrazena slovy "koncoví uživatelé". Bylo by nemožné, aby podnik získal souhlas od někoho, s kým nemá obchodní vztahy.

Slovo "zabezpečení" musí být nově definováno tak, aby jasně pokrývalo jak technickou bezpečnost, tak kybernetickou bezpečnost. "Dostupnost" sítí musí být rovněž zahrnuta do čl. 6 odst. 1. Zařízení třetích stran připojená k síti, která je zpřístupní prostřednictvím zpracování dat, by měla být také povolena (např. Směrovač). To by se mělo týkat i zařízení uživatelů.

Čl. 9 odst. 3 není nutný a měl by být vypuštěn. Právo na odvolání souhlasu kdykoli je již možné v rámci čl. 7 odst. 3 GDPR a mělo by se rovněž použít v souvislosti s tímto návrhem. Proto není nutné zavedení dodatečné povinnosti informovat koncové uživatele v pravidelných 6 měsíčních intervalech o jejich právu zrušit souhlas.

10) Opravné prostředky – SPČR chápe, že je důležité, aby uživatelé měli možnost při porušení svých práv využít nápravných opatření. V rámci článku 80 GDPR je to možné, včetně možnosti být zastoupena jinou neziskovou organizací.

Článek 21 nařízení o ePrivacy však zavádí zcela jiný systém - možnost využít nápravných prostředků podle tohoto článku se bude vztahovat na jakoukoli fyzickou nebo právnickou osobu jinou než uživatele, která byla nepříznivě ovlivněna případnými porušeními předpisů.

Článek 21 by měl být vypuštěn, protože výše zmíněné prostředky jsou v tomto ohledu již pokryty v GDPR. Místo článku 21 stačí jednoduchý odkaz na GDPR. Tento soulad s GDPR bude také znamenat větší právní jistotu pro podniky, které by v praxi fungovaly jak v rámci tohoto návrhu nařízení, tak v rámci GDPR.

Požadavky SP ČR

- Zapojení zástupců firem do debaty o dopadu nařízení na firmy a zejména na koncept Průmyslu 4.0na národní úrovni, včetně zapojení do procesu vytváření pozic ČR k tomuto návrhu.
- Odstranění OTT služeb, komunikace mezi stroji, doplňkových služeb a internetu věcí z dosahu nařízení (recitál 11 a 12).
- Přepracování článku 8, jehož současné znění by mělo zásadní negativní dopad na fungování digitální ekonomiky jako takové.
- Vypuštění zmíněných odstavců v článcích 6, 7, 9, 10 a 21.
- Zajištění souladu s GDPR a vymezení jasného vztahu těchto dvou nařízení.
- Posunutí plánovaného termínu nabytí účinnosti tak, aby vznikl dostatek prostoru pro konzultace s poskytovateli služeb a dalšími zainteresovanými firmami.