Institut pro digitální ekonomiku

Working Paper

Závěry z diskusi na workshopu 24. února 2016

Aktuální vývoj

Osobní údaje uživatelů jsou v současnosti pravděpodobně nejcennější komoditou digitální ekonomiky. Na rostoucí zájem o data reaguje i dlouhá léta připravovaná regulace Evropské unie. Na konci roku 2015 bylo úspěšně uzavřeno vyjednávání mezi Evropskou komisí, Parlamentem a Radou o podobě nového Obecného nařízení o ochraně osobních údajů (GDPR – General Data Protection Regulation). Tento předpis, který by měl nabýt účinnosti během dvou let, nahradí současnou právní úpravu ochrany osobních údajů v podobě směrnice 95/46/ES a, vzhledem k jeho přímé aplikovatelnosti, rovněž zákon č. 101/2000 Sb. Byť se jedná o nařízení, GDPR počítá s velkým množstvím prováděcích předpisů. Vzhledem k tomu hrozí podobně jako v případě směrnice rozdílnost národních úprav. Na druhou stranu ale GDPR obsahuje procesní mechanismus v podobě sjednocujícího orgánu – European Data Protection Board, který by měl tyto rozdílnosti jednotnou aplikací sbližovat.

Z hlediska právní jistoty je problém délka trvání přechodného období, než nový systém začne plně a předvídatelně fungovat, tedy než bude dostatečné množství závazných rozhodnutí (EDPB, SDEU, ÚOOÚ a dalších). Toto období by alespoň na národní úrovni mohlo být zkráceno, kdyby byl v ČR přítomný regulátor. Mezi zástupci trhu panuje shoda, že by měl být dříve, než za dva roky, kdy nabyde GDPR účinnosti. Není totiž vhodné, aby ÚOOÚ byl v roli pouhého řešitele stížností. Trh potřebuje na straně státu pro diskusi partnera s odpovídajícími pravomocemi. Proto panuje zájem na tom, aby byl zákon o regulátorovi pro ochranu osobních údajů co nejdříve. Současně je z důvodu specifické kompetence vhodná úprava služebního zákona pro regulátory.

V tomto přehledovém dokumentu je vybráno několik zásadních novinek, které budou mít významný vliv na praktické fungování celého systému ochrany osobních údajů. Dále jsou seřazeny do tří skupin dle jejich povahy.

Proces implementace v ČR

GDPR zatím není vládní prioritou. Česká republika ani neudělala veřejnou konzultaci a neaktualizovala svou pozici. Současně nemá zákon o DNA a ministerstvo vnitra to necítí jako důležité a jde cestou středoasijských republik. Historickým rozhodnutím vlády je ÚOOÚ v gesci ministerstva vnitra. S ohledem na rozsah agendy by se měli doplnit i další gestoři jako jsou ministerstvo průmyslu a obchodu, spravedlnosti a další. Rovněž předsedkyni ÚOOÚ by bylo vhodné přizvávat na jednání vlády.

Na trhu panuje nejistota, jak detailně se mají využívat nástroje ochrany osobních údajů, tedy jaké jsou detailní povinnosti správce. Klíčový je výklad ÚOOÚ, s ohledem na skutečnost že GDPR ponechává řadu výkladových nejasností ve zcela zásadních otázkách. Trh by měl sestavit příklady konkrétních příkladů, na které se GDPR bude vztahovat, včetně specifikace technologických řešení. Na základě těchto příkladů se může trh s ÚOOÚ a dalšími relevantními partnery na straně státu připravit na budoucí scénáře konkrétní aplikace GDPR. Chybí rovněž i základní informovanost vůči průmyslovým sektorům a diskuse s nimi o možných dopadech GDPR.

Trh musí při implementaci sehrát aktivní roli a poskytovat regulátorovi praktickou zpětnou vazbu k praktickým dopadům základních konceptů, jako je šíře definice osobního údaje, profilování, nakládání s online identifikátory či vyjadřování a způsob zajištění/poskytování souhlasu se zpracováním osobních údajů. Ve spolupráci s regulátorem tedy bude potřeba vyjasnit praktické otázky, jako například jaký způsob vyjádření souhlasu bude preferovaný, jak se bude ověřovat/dokazovat vynaložení odpovídajícího úsilí správce osobních údajů k ověření skutečnosti, že ke zpracování údajů dětí byl dán souhlas zákonným zástupcem, či jestli správce údajů použil/mohl použít k identifikaci fyzické osoby všechny objektivní faktory, nástroje a technologie dostupné v době posuzování ("*all the means reasonably likely to be used, such as singling out, to identify the individual directly or indirectly*"). Zajímavou otázkou budou i pseudonymizovaná data, na která trh sázel coby na možnou únikovou cestu z režimu ochrany osobních údajů, avšak která GDPR a regulátor ve finále stejně považuje za osobní údaje.

Při implementaci by mělo být pamatováno rovněž na předpisy týkající se kybernetické bezpečnosti, tedy zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) a chystanou Směrnici NIS.

1. Zpracování osobních údajů

a) Přísnější pravidla pro souhlas se zpracováním

Souhlas se zpracováním osobních údajů zůstává jedním ze způsobů, kterým může jejich správce legitimizovat plánované zpracování osobních údajů (čl. 6 GDPR). A to včetně zvláštních kategorií údajů[1] (čl. 9 GDPR). I pro GDPR platí, že základní vlastností platného souhlasu je, že je informovaný – tedy, že uživatel byl před jeho udělením srozuměn se zpracováním osobních údajů přijatelnou formou, které porozumí. Edukace populace je klíčovou součástí celé regulace.

[1] Dnes známé jako „citlivé údaje".

GDPR přináší jako novinku konkrétní úpravu bližší specifikace požadavků na souhlas se zpracováním (čl. 7). Požadavky v tomto článku uvedené nejsou zcela nové, protože se interpretačně daly dovodit již ze současné směrnice 95/46/ES, případně z výkladových materiálů Úřadu pro ochranu osobních údajů (ÚOOÚ) a Pracovní skupiny zřízené dle článku 29 (WP29).[2] GDPR klade na správce údajů vyšší nároky požadavkem na větší vstřícnost vůči subjektům údajů během procesu získání jejich souhlasu. Konkrétně pak následujících podmínek:

- Pokud je souhlas se zpracováním součástí jiného dokumentu (smlouvy), musí být zřetelně oddělen, aby nevznikl pocit, že smlouvu není možné uzavřít bez udělení souhlasu;[3]
- Při popisu zpracování za účelem získání souhlasu musí být použit prostý a srozumitelný jazyk;
- Subjekt údajů má možnost souhlas kdykoli odejmout (a to stejně snadno, jako jej udělí) a musí být o této možnosti informován;
- Souhlas je platný jedině, pokud je udělen svobodně, tedy bez rizika neposkytnutí služby, nebo zhoršení situace subjektu údajů.[4]

Povinnost správce údajů být schopen prokázat existenci souhlasu po celou dobu probíhajícího zpracování zůstává zachována.

Novinkou v rámci interpretace je výslovné zmínění online identifikátorů a jejich příkladů v recitativu nařízení a nahlížení na ně coby na osobní údaje. V kombinaci s výkladovou nejasností definice osobních údajů (za jakých podmínek bude daný identifikátor považován za osobní údaj) na straně jedné a podstatu a rozsah využívání online identifikátorů na straně přivádí trh do právní nejistoty.

Novinkou je specifické pravidlo, které stanoví, že souhlas se zpracováním osobních údajů subjektu mladšího 16 nebo 13 let[5] může být udělen jen jeho zákonným zástupcem. Osobní údaje zpracované tímto způsobem pak bez dalšího spadají do režimu údajů, jejichž výmaz je možné požadovat na základě práva na výmaz (na zapomnění) dle čl. 17.[6] Není však prakticky jasné, jak se souhlas rodičů za tyto nezletilé bude v praxi poskytovat, případně kontrolovat jeho poskytnutí.

Zároveň ale stále platí, že souhlas se zpracováním je jen jedním z legitimizačních důvodů pro zpracování osobních údajů a měl-by být správně využíván spíše střídmě, protože ve

[2] Poradní orgán Komise pro oblast ochrany osobních údajů sestávající se ze zástupců národních úřadů pro ochranu osobních údajů.
[3] Zpracování údajů za účelem plnění smlouvy je v GDPR, stejně jako dnes, zvláštní legitimizační důvod.
[4] Tento požadavek je platný již nyní, byť není tak jasně formulovaný.
[5] Bude záviset na národní legislativě.
[6] Viz dále.

většině případů není potřeba. Je totiž možné aplikovat další legitimizační důvody – např. zpracování za účelem plnění smlouvy, oprávněný zájem správce, nebo plnění zákonné povinnosti. Např. ČTÚ u subjektů, které reguluje, zaznamenal užívání specifických souhlasů při podpisech smluv (kontakty v infolinkách, další souhlasy, informace o pokutách apod.) a zabývá se oprávněnou obavou, že lidé souhlasy z důvodu jejich komplikovanosti či rozsáhlosti nečtou.

b) Únikové klauzule

Únikové klauzule z povinností, kde není možné jejich plnění je novinkou GDPR, která nepřidává správcům údajů žádné nové povinnosti. Je zmíněna jako příklad toho, že se nová právní úprava snaží reflektovat nedostatky současné směrnice 95/46/ES, která již v mnoha oblastech nestačí na rychle se rozvíjející technologie a vyžaduje plnění povinností tam, kde to není v reálné praxi možné.[7]

Čl. 10 GDPR zavádí výjimku, podle které, pokud pro účel zpracování osobních údajů není nutná další identifikace subjektu údajů, správce tuto identifikaci nemusí získat, aby splnil povinnosti z GDPR. Druhým takovým příkladem je čl. 14a odst. 4 písm. b), který zavádí výjimky z obecné povinnosti informovat subjekt údajů pro případy, kdy by poskytnutí informace o zpracování bylo nemožné, nebo představovalo nepřiměřené úsilí.

c) Právo na výmaz (zapomnění)

Nově formulované právo, (často diskutované po rozhodnutí Soudního dvora EU ve věci Google Spain), které vychází ze současného práva subjektu údajů požadovat zanechání zpracování údajů, které nejsou odpovídající účelu jejich zpracování. Čl. 17 a 17a GDPR vymezují následující situace, kdy subjekt údajů může požadovat zanechání zpracování jeho osobních údajů a jejich výmaz:

- Údaje nejsou nezbytné vzhledem k účelu zpracování, pro které byly sesbírány, nebo zpracovávány;
- Subjekt odejme souhlas se zpracováním a správce nemá žádný jiný zákonný důvod pro zpracování údajů;
- Subjekt údajů namítá zpracování osobních údajů dle čl. 19 GDPR;[8]
- Údaje byly zpracovávány protiprávně;
- Údaje mají být vymazány za účelem splnění právní povinnosti;
- Údaje byly sbírány a zpracovávány na základě souhlasu zákonného zástupce;

Pokud dojde na základě některého z výše uvedených důvodů k vymazání údajů, které správce[9] uveřejnil, má rovněž povinnost podniknout přiměřeně nezbytné kroky k tomu, aby

[7] Jako příklad může sloužit povinnost informovat subjekt údajů o probíhajícím zpracování, která v případě správce, jako je internetový vyhledávač ve smyslu rozhodnutí Google Spain, není naplnitelná.

[8] Namítat zpracování je možné v případech, kdy je zpracování prováděno na legitimizačním základě veřejného zájmu a oprávněného zájmu správce dle čl. 6/ odst. 1 písm. e, f.

o požadavku subjektu údajů informoval další osoby, které tato data zpracovávají. Článek 17 odst. 3 pak uvádí několik výjimek, kdy se právo na výmaz neaplikuje (např. pokud by tím mělo být zasaženo do práva svobody projevu). Rozdíl znění v GDPR, oproti tomu, jak je chápáno v souvislosti s rozhodnutím Google Spain, spočívá v tom, že dle GDPR právo na výmaz cílí rovněž na původní správce údajů – autory zdrojových internetových stránek, které internetové vyhledávače indexují.

Toto právo je jedno z řady nově výslovně vyjádřených práv subjektu údajů, které správci budou nuceni vzít v potaz a vyhradit zdroje pro jejich naplňování.

2. Nové povinnosti správce související s bezpečností údajů

V této části je vybráno několik zásadních nových povinností, které bude muset správce údajů plnit v souvislosti se zajištěním zabezpečení zpracování osobních údajů. Oproti směrnici 95/46/ES ubyla povinnost registrace správce údajů u národního orgánu ochrany osobních údajů. Na druhou stranu ale zase přibyla povinnost provádět v určitých případech hodnocení dopadů plánovaného zpracování osobních údajů a zřízení pozice tzv. inspektora osobních údajů.

a) Ochrana By Design & By Default

„Data protection by design" úzce souvisí se zásadou tzv. minimalizace údajů. Na pozadí tohoto principu, který budou mít správci nově povinnost dodržovat, stojí myšlenka, že je mnohem efektivnější (jak funkčně, tak ekonomicky), pokud je s ochranou osobních údajů počítáno již od počátku návrhu praktického řešení jejich zpracování.[10] Může se jednat jak o technická řešení typu anonymizace, pseudonymizace a rozdělení (ať už fyzické, nebo logické) oblastí s uloženými daty. Nebo personální a organizační opatření (kdo ze zaměstnanců správce údajů má přístup k jakým údajům, jaké jsou toky dat v rámci společnosti atd.).

Princip „data protection by default" pak má zajistit, aby v základním nastavení služby byly zpracovávány jen osobní údaje, které jsou zcela nezbytné pro její poskytování. Tento princip pak zřejmě míří primárně na zpracování osobních údajů při nabízení služeb online.

Je třeba si uvědomit, že tyto zásady se budou týkat všech průmyslů, tedy nejen IT technologií. Rovněž sílí tlak na byrokratizaci ochrany osobních údajů a zabezpečení. Bude zcela na rozhodnutí trhu, kde aplikovat svobodné certifikace a audity. Odpovědnost je zcela na bedrech správců údajů. Velice často si neuvědomují, že chtějí-li si například držet svá

[9] Obecně se povinnosti zde uváděné týkají jak správce, tak zpracovatele osobních údajů.

[10] Ve zkratce můžeme říci, že je snadnější technické a další prostředky ochrany soukromí a osobních údajů vložit do systému při jeho vzniku, než je později „přišívat" k již hotovému.

data v cloudu, znamená to pro ně rozsáhlé povinnosti v oblasti ochrany osobních údajů a zajištění jejich bezpečnosti. Přejímají totiž odpovědnost i za své nasmlouvané zpracovatele.

b) Bezpečnost zpracování a ohlašování případů narušení bezpečnosti (Data Breach)

GDPR klade na správce požadavek zajistit za pomoci technických a organizačních prostředků bezpečnost zpracování osobních údajů. Čl. 30 GDPR výslovně uvádí, že při poměřování nezbytné míry zabezpečení je třeba brát v potaz na jedné straně náklady nezbytné pro zajištění takových prostředků a na straně druhé povahu zpracovávaných osobních údajů a riziko možných dopadů jejich případného zničení, úniku, nebo nezákonného zpracování. V tomto smyslu GDPR navazuje na směrnici 95/46/ES.

Novinkou je ohlašovací povinnost v případě narušení bezpečnosti zpracování osobních údajů („(personal) data breach"). Správce má povinnost bez odkladu, nejpozději však do 72 hodin, incident ohlásit DPA[11], do jejíž jurisdikce náleží. Tato lhůta je pro umožnění reagovat na incident a pokusit se ho vyřešit. Správce údajů může dostat pokutu i za to, že to nezjistil, že došlo k narušení bezpečnosti dat. Čl. 31 GDPR pak stanoví, že v případě, že by důsledkem data breach bylo vysoké riziko zásahu do základních lidských práv a svobod subjektu údajů, má správce povinnost informovat jej o incidentu, a to bez zbytečného odkladu. Při hlášení má správce údajů povinnost popsat například charakter incidentu, možná rizika a kroky, které byly podniknuty pro jeho odvrácení.

ÚOOÚ vytvořilo zvláštní tým s cílem být připraven na ohlašování narušení bezpečnosti zpracování osobních údajů, nicméně dosud byly nahlášeny pouze dva případy ročně. České republice dosud chybí jednotné místo pro oznamování Data Breach – zejména proto, že různé předpisy pracují s tímto termínem trochu odlišně. Existuje však předběžná dohoda ÚOOÚ s NBÚ, který je schopen během jedné hodiny napsat výzvu a stížnost.

Správci údajů budou mít motivaci hlásit data breach ve vazbě na možné reputační riziko či sankce. Zákon v zájmu limitace rizika poškození dobrého jména obsahuje úpravu, že ÚOOÚ může zveřejňovat a předávat pouze poznatky obecné (nikoli tedy detaily konkrétního případu narušení bezpečnosti dat), a rovněž není možné zveřejňovat údaje od třetí osoby. I v této oblasti bude velice klíčová role inspektorů osobních údajů, kteří budou fungovat jako prostředník mezi správcem údajů a ÚOOÚ ke konzultaci otázek běžných i krizových.

Správcům údajů by měla být ponechána procesní a technologická volnost při zajištění bezpečnosti dat vlastních uživatelů. Určitý problém však spočívá v tom, že v řadě případů budou navíc "data breaches" schopny zaregistrovat a odhalit pouze firmy, které mají kvalitně nastavenou a zajištěnou ochranu dat svých uživatelů. Tuto skutečnost je třeba brát v potaz a zabránit skutečnosti, kdy se firmy budou bát komunikovat s odpovědným úřadem z důvodu jejich ostrakizace/možné negativní mediální kampaně.

[11] Data Protection Authority, v českém případě jde o Úřad pro ochranu osobních údajů.

c) Posuzování dopadu na ochranu údajů

Článek 33 GDPR zavádí povinnost vypracovat posouzení dopadů plánovaného zpracování osobních údajů. A to v případech, kdy vzhledem k povaze jejich zpracování[12] hrozí vysoké riziko zásahu do základních práv a svobod subjektů údajů. Jako příkladný výčet zpracování, k nimž by mělo být posouzení dopadů vypracováno, odst. 2 uvádí:

- Profilování;
- Zpracování velkého množství citlivých údajů;
- Systematické monitorování veřejného prostoru.

DPA může stanovit seznam druhů zpracování osobních údajů, pro které je vypracování posouzení dopadů povinné.

Čl. 34 GDPR dále stanoví, že správce údajů má v případech, kdy z posouzení dopadů vyplyne vysoké riziko zásahu do základních práv a svobod subjektů údajů, povinnost před zahájením zpracování konzultovat následný postup s DPA, do jejíž jurisdikce spadá. DPA pak v kooperaci se správcem údajů zajistí, aby nedošlo k nezákonnému zpracování osobních údajů.

d) Jmenování inspektora ochrany údajů

Správce údajů má povinnost jmenovat inspektora osobních údajů (formou zaměstnaneckého poměru, nebo dohody o externí spolupráci).[13] To platí v případech kdy:

- Zpracování je prováděno orgánem veřejné moci;
- Hlavní činnost správce spočívá ve zpracování údajů v podobě pravidelného systematického monitorování velkého množství subjektů údajů;
- Hlavní činnost správce spočívá ve zpracování velkého množství citlivých údajů;
- Další případy, kdy je jmenování inspektora nezbytné pak může určit národní právo.

Více správců se pak může domluvit, že budou společně využívat služeb jednoho inspektora. Ten má být vybrán a jmenován na základě svých profesních kvalit a zkušeností a má mít poměrně silnou a nezávislou pozici v rámci struktury správce údajů. Čl. 36 GDPR stanoví, že inspektor přímo odpovídá nejvyššímu vedení správce údajů, má mu být umožněno vykonávání jeho povinností vyplývajících z GDPR a nesmí být propuštěn, nebo penalizován za to, že tyto povinnosti plní. Inspektor pak má fungovat jako prostředník mezi správcem údajů a DPA a mohou se na něj přímo obracet subjekty údajů.

Existuje obava trhu, že inspektora ochrany osobních údajů bude muset mít každý podnik, který pracuje s cookies. Na konkrétní způsob provedení aplikace zmiňovaného ustanovení však budeme muset nejprve počkat. Správci údajů, kteří již mají experta na data a datovou bezpečnost, mohou těmto pracovníkům pouze rozšířit pravomoc i na ochranu osobních

[12] Zejména v souvislosti s užitím nových technologií.
[13] Čl. 35.

údajů. ÚOOÚ věří, že v České republice převáží německý model, kdy podniky budou využívat třetí subjekt, který je uvede do problematiky. Dokonce existují už dodavatelé e-shopů, kteří nabízejí v rámci služby e-shopu i službu "inspektora osobních údajů", takže si ji klient objedná spolu s e-shopem.

Co se týče obav trhu z možných kontrol, již dnes jsou kontroly avizovány v dostatečném předstihu a firmy tedy budou mít čas se na ně připravit. Krom toho, již dnes mohou správci údajů navrhnout první příklady toho jakou podobu činnosti a výstupy inspektorů osobních údajů mohou mít a tento návrh předložit ÚOOÚ. Mohou se tak aktivně podílet na zformování praktického stavu, který zavládne po účinnosti GDPR.

3. Předávání údajů do zahraničí

Zejména v souvislosti s rozhodnutím Soudního dvora Evropské unie ve věci Schrems je v poslední době hojně diskutovaný problém předávání osobních údajů do zahraničí. Úprava GDPR navazuje na současnou úpravu dle směrnice 95/46/ES. Předpokládá následující právní důvody pro předávání osobních údajů do zemí mimo EU:

- Rozhodnutí Komise o adekvátní úrovni ochrany (čl. 41);
- Předávání při existenci potřebných opatření pro zajištění úrovně ochrany (čl. 42);
- Binding corporate rules (čl. 43);
- Specifické případy předávání údajů uvedené v čl. 44 jako jsou například:
    - Výslovný souhlas subjektu údajů s předáním do třetí země;
    - Předání je nezbytné pro splnění smlouvy mezi správcem a subjektem údajů;
    - Předání je nezbytné pro důležitý veřejný zájem;
    - Ve velmi omezeném a přísném režimu, předání je nezbytné pro naplnění oprávněného zájmu správce údajů.

Je vhodné zdůraznit, že co se týče kauzy Schrems a tedy předávání údajů do USA, není možné říct, že celá stávající úprava je špatná. Nově vyjednaný Privacy Shield, který nahrazuje institut bezpečného přístavu, ze současného stavu hodně vychází a nabízí nové pojistky ochrany zejména na úrovni americké vlády. Pro správce, kteří naplňovali podmínky Bezpečného přístavu, tedy bude přechod do nového režimu bezproblémový.

Pro Českou republiku může být problematické předávání osobních údajů do zemí, se kterými obchoduje, ale u kterých nebylo vydáno rozhodnutí Komise o adekvátnosti ochrany. Otázka předávání údajů do takových zemí, a tedy usnadnění obchodu s nimi, by měla být na národní úrovni intenzivněji řešena. Příkladem může být Jižní Korea v kontextu leteckého dopravce či další investoři a podniky, působících v naší zemi.

4. Procesní otázky a mezinárodní aspekt

Aby GDPR splnilo sjednocovací funkci, obsahuje v sobě ustanovení zavádějící silný centrální evropský orgán ochrany osobních údajů – European Data Protection Board. Tento orgán vznikne ze současné pracovní skupiny WP 29 a na rozdíl od ní bude mít rovněž rozhodovací pravomoc. Předpokládá se tedy jeho značná aktivní role a to zejména v případech, kdy bude třeba řešit kompetenční spory mezi jednotlivými úřady členských států. Na postupu při tvorbě rozhodnutí, která se budou týkat jiných státu (v případě ČR např. Slovenska, kde mají české firmy řadu datových center), se budou muset shodnout kompetentní úřady v daných členských státech. V případě, že ke shodě nedojde, rozhodne právě European Data Protection Board. Doposud není známá podoba prováděcích předpisů ze strany Evropské Komise. S ohledem na vytváření jednotného digitálního trhu a k tomu se vážící stoupající přeshraniční aspekt je zároveň otázkou, jak bude probíhat spolupráce a vymezování pravomocí mezi jednotlivými národními regulátory na straně jedné a role, či ambice Data Protection Boardu (a EK) na straně druhé. Jedná se o málo komunikovanou, leč potenciálně problematickou skutečnost.

V otázce mezinárodních korporací se aplikuje pravidlo one-stop-shop, tedy dostačující se jedno zastoupení mezinárodní korporace v jedné zemi EU. Přesto má občan právo řešit ve svém případě regulaci ve své vlastní zemi. Otázky specifických zemí (např. jako Facebook, registrovaný v Irsku) bude řešit Data Protection Board. Otázka je, jak složitý tento proces bude. Soudní kauzy naznačují, že institucionální ochrana zatím nezajišťuje to, co právo nabízí uživatelům. Ovšem je právě ambicí GDPR tento stav napravit.

Další otázkou je aplikovatelnost GDPR, respektive vymáhání povinností z něj plynoucích, na mimoevropských správcích údajů, kteří v EU nemají zastoupení, ale do EU distribuují produkty, služby, nebo monitorují chování subjektů údajů v EU. Spadají tedy pod působnost GDPR na základě čl. 3 odst. 2. Vzhledem k obtížnému prosazování práva na takovýchto správcích mohou být evropské firmy v konkurenční nevýhodě z důvodu svých zákonných povinností. Jde například o souhlasy, které mimoevropské služby nemusejí zobrazovat. Do konkurenční výhody se tyto mohou dostat i z důvodu neadekvátně prosazovaných informačních povinností (a jejich rozsahu) a forem jejich grafického zobrazování, kdy povinnost prezentovat informační bannery v množství a formě snižujících uživatelský komfort může v krajním případě vést k přechodu k jiné, mimoevropské službě.