Z domova

Nová ochrana osobních údajů: co přinese lidem

1 Chtějí mít vaše data? Musí vás nově požádat

Doteď udělené souhlasy s užíváním telefonních čísel či mailů pro marketingové účely přestávají platit. Firmy, které databáze mají, musí klienty požádat znovu. Mělo by tak ubýt nevyžádaných hovorů.

2 Vaše „ano“ musí být ve smlouvě jasně viditelné

Už žádné zanoření souhlasu s využíváním osobních údajů hluboko ve smlouvách či obchodních podmínkách. GDPR vyžaduje, aby souhlas byl od zbytku dokumentů oddělený. Každý zákazník musí jasně vidět, na co kývá. Musí být srozumitelně popsáno, na co firma jeho údaje použije.

3 Mlčení už neznamená souhlas

Souhlas s použitím osobních údajů musí být aktivní, například zaškrtnutí políčka na webu.

4 Méně úniků citlivých údajů za cenu obřích pokut

Obří pokuty, které se mohou šplhat i nad půl miliardy korun, by měly firmy nutit zacházet s hesly či maily výrazně opatrněji. Scénářů, kdy se citlivá data hackerů dostanou na web, by mělo být výrazně méně.

5 On-line přístup k databázím

K osobním údajům, které firmě dotyčný poskytne, by měl mít přístup, nejlépe napřímo a on-line. Tajné databáze s výjimkou například bezpečnostních složek nepřipadají v úvahu.

6 Právo na zapomnění

Firmě, která jeho osobní data využívá, to bude mít člověk právo zakázat. Takzvané právo na zapomnění, tedy právo na vymazání osobních dat, půjde uplatnit třeba vůči sociálním sítím. GDPR zároveň zaručuje uživatelům i možnost svá data si vyžádat a jednoduše přestěhovat od jednoho provozovatele k druhému. Třeba tak přejít z jedné služby na druhou, například sociální síť.

Co znamená GDPR?

Obecné nařízení o ochraně osobních údajů (angl. General Data Protection Regulation)

Anketa Jak se připravujete na novou ochranu osobních dat, která začne platit v květnu. Kolik vás to bude stát a jaká je největší komplikace?

Billa
Dana Bratanková, mluvčí společnosti

„Pro zajištění nových souhlasů klientů se zpracováním jejich dat využijeme webové rozhraní a tištěný formulář na prodejnách. O změně věrnostního programu neuvažujeme. Na úpravy vynaložíme miliony.“

Košík.cz
Jakub Šulta, šéf společnosti

„Uvedení předpisu do praxe je pro nás spíše formální záležitostí. Od zákazníka chceme pouze informace, které využíváme pro zlepšení naší služby. Požadujeme jen nezbytné minimum informací.“

Clever Monitor
Kristýna Vlčková, ředitelka strategického rozvoje

„GDPR je pro mnohé velký strašák. Platí, že firmy, které už nyní důsledně dodržují současnou legislativu, mají s přípravou nové směrnice méně práce. Naše náklady se pohybují okolo 700 tisíc korun.“

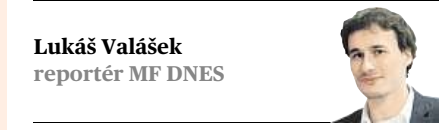
Amper Market
Jan Maňas, mluvčí společnosti

„Je to pro nás velká neznámá. V současné době pracujeme na konkrétních opatřeních a doufáme, že to stihneme. Směrnice bude vnímána spíše jako nepříjemné byrokratické opatření.“

Foto: Shutterstock

Soukromí pod zámkem

Ochrana dat klientů je dnes hlavně na papíře: v praxi moc nefunguje. Od května ji má zajistit hrozba likvidačních pokut pro firmy i obce.



Lukáš Valášek
reportér MF DNES

Když před Vánocemi z internetového bazaru hlavního města uniklo 35 tisíc e-mailů a hesel, Pražané, jimž údaje patřily, se to dozvěděli až z novin. Měsíc a půl potom, co o útoku hackerů informoval provozovatele stránek jeden z bezpečnostních expertů. Mezitím ukradená hesla, která mnoho lidí používá stejná napříč internetem, mohl kdokoliv zneužít.

Podobnému tutlání útoků hackerů už by měl být konec. Nová legislativa EU totiž nařizuje, aby firmy či instituce, kterým osobní údaje uniknou, nejpozději 72 hodin od okamžiku, kdy se o incidentu dozvědí, vše nahlásily Úřadu pro ochranu osobních údajů. A v mnohých případech musí obratem rovnou informovat přímo i ty, kterým osobní údaje patřily. Ti pak mohou reagovat – změnit si hesla či pozorněji hlídat, jestli se jim někdo nepokouší ukrást virtuální identitu.

„Nařízení má cílit hlavně na ty, kteří ve velkém obchodují s naším soukromím. Nová pravidla reagují na narůstající rizika zneužívání, úniků a zpeněžování osobních dat Evropanů, která přinesla digitální éra,“ popsala česká eurokomisařka Věra Jourová (ANO), která je za pravidla odpovědná. Nové nařízení pod zkratkou GDPR začne platit 25. května na území celé Unie. Na 88 stranách obecně formuluje, co musejí všechny firmy, které nakládají s osobními údaji evropských občanů dodržet, aniž by to do zákonů musely začlenit jednotlivé státy.

A nejsou to jen prázdné deklamace. EU totiž výrazně nafoukla pokuty, které za únik osobních dat jednotlivým firmám hrozí. Když předloni operátorovi T-Mobile v Česku unikly citlivé údaje od více než milionu klientů, dostal za to pokutu 3,6 milionu korun. Byla to nejvyšší sankce, jakou Úřad pro ochranu osobních údajů kdy udělil. Dnes by mu za stejný prohřešek hrozila pokuta až 20 milionů eur, tedy více než půl miliardy korun. Nebo dokonce až 4 procenta celosvětového obratu.

„Úřad považuje za prokázané, že společnost nepřijala dostatečná opatření k zabezpečení osobních údajů obsažených v elektronické interní databázi. V důsledku toho došlo k odcizení uvedených dat jejím zaměstnancem,“ zdůvodňoval tehdy sankci pro T-Mobile mluvčí úřadu David Pavlát. A ten se kál, že do budoucna výrazně zpřísní bezpečnostní opatření.

Právě vyšší pokuty jsou podle expertů zásadní součástí GDPR, která by firmy mohla donutit se o své citlivé databáze lépe starat. Bezpečnostní opatření jsou totiž nejenom drahá, ale zároveň mohou zaměstnancům komplikovat práci, a tím i snižují jejich výkonnost. Některým firmám se tak do nich příliš nechtělo. I když fakticky povinnost maximálně hlídat data mají ze zákona už nyní.

„Říká se, že kdo dodržoval nyní platný zákon na ochranu osobních údajů, tak se nemá s příchodem GDPR čeho obávat. Skutečnost je však taková, že ho téměř nikdo nedodržoval. Také to bylo způsobeno tím, že pokuty byly úplně někde jinde a lidé se moc nezajímali o to, kdo co o nich zpracovává,“ popsal Michal Nulíček z advokátní kanceláře Rowan Legal.

Citlivé údaje k ukradení

Podobné úniky, jako jsou ty, které postihly webový bazar pražského magistrátu, přitom zasáhly v posledních letech mnohé české společnosti. Hackeři pak data nabízejí v obřích balících k prodeji na internetu.

Jestli e-mail či heslo volně leží na webu, si přitom může zkontrolovat každý sám. Bezpečnostní expert Troy Hunt na to provozuje speciální web haveibeenpwned.com. Do vyhledávacího políčka na stránce stačí zadat svůj mail nebo heslo.

Hunt do obří databáze nahrává jednotlivé úniky. Souhrnně takto dohledal už téměř 5 miliard uživatelských účtů lidí z celého světa. Zaskočeno takto může být třeba až 700 tisíc zákazníků českého e-shopu mall.cz, kterému vloni unikly nejenom e-maily a hesla, ale i telefony či jména zákazníků. V Huntově databázi je to největší ryze „český“ únik. Firma argumentovala, že šlo o zastaralé údaje z roku 2015 a dřívější.

Odborníci však podtrhávají, že těm, kteří nezodpovědně pumpují svá citlivá data, fotografie nebo hesla do neprověřených služeb, nové nařízení nebude nic platné. „Na jedné straně chráníme, co na druhé vykřikujeme,“ argumentuje advokátka a bývalá ministryně spravedlnosti Daniela Kovářová.

GDPR dává lidem právo další využívání osobních údajů zakázat a nařídit jim jejich smazání, pokud i zpětně získají pocit, že je někdo využívá nevhodně nebo je špatně chrání. Výjimkou jsou závažné, prokazatelné důvody k uchovávání dat. Co přesně to bude znamenat, zatím není příliš jasné. Právě za přílišnou obecnost, která je pro legislativu značně netypická, kritizují GDPR experti.

„Ptala se mě například jedna lékařka, která má psychiatrickou ambulanci, co to pro ni bude znamenat. Má chorobopisy pacientů, u nichž jsou uvedena choulostivá data, která jí při vyšetřeních sdělují. Co když jí řeknou, že je chtějí vymazat?“ uvádí jeden z příkladů místopředseda Nejvyššího soudu Roman Fiala.

Soudce: Lékaři se bojí, že musí mazat chorobopisy

Nový způsob ochrany osobních dat podle nařízení Evropské unie, takzvané GDPR, má fungovat už od 25. května. Nikdo přitom ještě neví, co to v praxi bude znamenat. Podle místopředsedy Nejvyššího soudu Romana Fialy je totiž velký problém v tom, že zatím není dokončený příslušný prováděcí zákon.

Jak dopadne GDPR na občana a jak na podnikatele, který s údaji pracuje?
Problém je v tom, že to vlastně nikdo neví. Vzniklo nařízení Evropské unie, které stanovilo pravidla, ale jen těmi nejobecnějšími formulacemi. Pro nás je to o to složitější, že teprve teď je v legislativním procesu vnitrostátní prováděcí zákon. Takže nařízení sice umožnilo každému národnímu státu, aby si specificky upravil vnitřní poměry pro podmínky konkrétní země, ale my jsme to zatím neudělali.

Přitom předpis má platit už za necelé tři měsíce...
Ano, takže je dost pozdě. Nedivím se, že narůstá nervozita. Ptala se mě například jedna lékařka, která má psychiatrickou ambulanci, co to pro ni bude znamenat. Má chorobopisy pacientů, u nichž jsou uvedena choulostivá data, která jí při vyšetřeních sdělují. Co když jí řeknou, že je chtějí vymazat? Pro ni je to nepředstavitelné. Znepokojovat se začala i média, protože nevědí, co je ta hranice, kdy shromažďují informace pro profesionální účely a kdy už ne. Proto některé národní státy novináře vysloveně vyňaly z režimu GDPR nebo minimalizovaly jeho dopad do novinářské praxe. U nás zatím nevíme, jak to bude. Předloha zákona na novináře nepamatuje.

Můžete dát konkrétní příklad, kdy by novinář mohl mít problém?
Dnes nikdo na otázku konkrétního případu neodpoví. Všichni jsme v nejistotě. Ti, kdo nakládají s těmito daty, jsou na jedné straně ujišťováni, že nařízení předpokládá až drakonické pokuty, ale na druhou stranu se říká, že nebudou ukládány. Ale mohu věřit tomu, že mi nebude uložena pokuta? To asi stěží. Dokud mi nebude uložena a dokud soud neřekne, že je to nesmyslná pokuta, tak jsem v nejistotě.

Soud se nebude řídit tím, že se někdy něco říkalo...
To nebude. Je mnoho protichůdných tendencí. Na jedné straně je tendence zveřejňovat veškeré možné údaje, prezentovat údaje o veřejně činných osobách, o daňových přiznáních a majetku. Dokonce lidé sami necítí problém zveřejňovat údaje o sobě na sociálních sítích. A proti tomu jde GDPR, které se snaží tyto údaje co nejvíc ochránit, což se může jevit jako logické, ale na druhou stranu to může být zcela proti jiné obecné tendenci.

Je samotné nařízení zpracované dobře?
Je udělané tak, aby bylo použitelné ve všech státech, to znamená velice obecně. Nereaguje – logicky – na zvláštnosti jednotlivých národních států. Mám ale pochybnost, jestli je správné to takto dělat. Vůbec si nejsem jist, zda to byl tak velký problém, že se vůbec mělo do GDPR jít.

Jaká mohla být motivace? Třeba ochrana osobních údajů na sociálních sítích?
Mohlo to být cokoli. Od snahy domoci se toho, že člověk může být zapomenut na sociálních sítích, až po cokoli jiného. Může to být i věc mého oblíbeného tématu, módy v právu. Jako je móda zveřejňování, je móda utajování, kam patří právě GDPR.

Má GDPR nějaké plus?
Jedno plus může být právě u sociálních sítí. Pokud tam někdo nerozvážně zveřejní své soukromé údaje, tak snad, zdůrazňuji snad, bude moci být díky GDPR na sociálních sítích zapomenut. – **Ivana Faryová**