Ochraně osobních dat se Češi stále učí

Před účinností evropského nařízení se na ochranu osobních dat v Česku příliš nehledělo. Nová pravidla správce dat štěpí. Některé ženou do absurdit.

Před rokem se české podniky a státní instituce vzpamatovávaly z paniky, kterou vyvolalo evropské nařízení o ochraně osobních údajů známé pod zkratkou GDPR. Na poslední chvíli se snažily dohnat *„resty“*. Rok poté řada z nich odložila ochranu osobních údajů na vedlejší kolej a nechce už do ní jakkoliv investovat.

„Jde o další příklad zcela zbytečného bruselského nařízení, které jen způsobilo obrovské množství zmatku, aniž by něco užitečného přineslo,“ říká například generální ředitel developerské společnosti Ekospol Evžen Korec. *„Právníci a všemožní konzultanti se najedli a my musíme makat o trochu více,“* myslí si Martin Lipert, zakladatel prodejce elektronických knih eReading.cz.

Obdobné názory na nařízení přitom nejsou mezi českými podnikateli nijak výjimečné. Hlavně u menších společností, které za sebou nemají aparát právníků, je pak ve vztahu k ochraně osobních údajů běžná naprostá rezignace. *„Tvrdí, že mají mnohem více úkolů k řešení a nemají šanci vyhovět,“* popisuje viceprezidentka Svazu průmyslu a dopravy ČR Milena Jabůrková. K takovému vnímání evropského nařízení podle ní přispěla mimo jiné příliš složitá, různorodá nebo nepoužitelná doporučení v médiích, na různých seminářích a vzdělávacích akcích.

Výsledkem rezignace a odmítavého přístupu je, že řada společností má v práci s osobními údaji velké rezervy. Březnový průzkum společnosti Cisco tak například ukázal, že požadavky vyplývající z nařízení splňuje úplně či z větší části jen 59 procent podniků. A podobně vyznívá i čerstvý průzkum poradenské společnosti KPMG, který na konferenci Osobní údaje 2019 – GDPR rok poté, pořádané vydavatelstvím Economia, představil partner KPMG Martin Hladík. Průzkum analyzoval, jak je na tom s dodržováním nových pravidel 52 významných českých společností od bank přes pojišťovny a operátory až po dopravce a energetické společnosti. Prohřešků proti nařízení odhalil 76.

Nejlépe v průzkumu KPMG dopadly banky a pojišťovny. Naopak nejvíce prohřešků či nejasností poradci našli u sportovních organizací a nemocnic. *„Fakultní nemocnice dlouho neřešily GDPR vůbec. Čekaly na pokyny z ministerstva zdravotnictví. V momentě, kdy je dostaly, je všechny jak přes kopírák zavedly,“* říká Hladík. V rozporu se stávajícími předpisy jsou zejména v oblasti zpracování cookies, tedy ukládání informací o návštěvnících svých webů. *„Fakultní nemocnice používají cookies, sledují, co dělají návštěvníci na jejich webu, ale nemají tam souhlas se zpracováním cookies ani informaci, že je používají,“* upozorňuje Hladík.

Obecně se podle něj jako problematické ukázalo také to, jak čeští správci a zpracovatelé dat plní informační povinnost, kterou podle nařízení mají vůči zákazníkům. *„Šlo o nejasně vymezený rozsah osobních údajů, které podniky zpracovávají, vymezení účelu, pro který je drží, a doby, po kterou je drží,“* popisuje Hladík. Chyby KPMG našlo také ve způsobu, jakým podniky sbírají souhlasy se zpracováním zákaznických dat, nebo v tom, jakým způsobem u nich mohou lidé uplatnit práva, která podle nových pravidel mají.

Nejlépe se podle průzkumu KPMG na nová evropská pravidla ochrany osobních údajů adaptovaly banky a pojišťovny. Naopak nejvíce prohřešků či nejasností poradci odhalili u sportovních organizací a nemocnic.

Foto: Zbyněk Pecák

Na konferenci Osobní údaje 2019 – GDPR rok poté vystoupili (zleva) partner poradenské společnosti KPMG Martin Hladík, partner advokátní kanceláře Rowan Legal Michal Nulíček, vedoucí analytického oddělení Úřadu pro ochranu osobních údajů Soňa Matochová a právník Coca-Coly Jan Kubíček.

Martin Hladík z KPMG účastníky konference seznámil s průzkumem, podle něhož se na evropská pravidla ochrany osobních údajů nejlépe adaptovaly banky a pojišťovny. Naopak nejvíce nedostatků je u sportovních organizací a nemocnic. Jan Kubíček z Coca-Coly (na fotografii vlevo) upozornil, že zákazníci se o ochranu svých dat příliš nezajímají. Za celý rok Coca-Cola řešila jen čtyři žádosti o výmaz zákaznických dat z databází. Dotazy na práci s daty téměř nedostává.

Typicky největší problém bývá s výmazem dat. *„Většina firem se nedokáže zbavit údajů, které už dávno nemá mít, a nastavit způsob, jak data průběžně vymazávat, když od nich klient odchází,“* popisuje Hladík.

Za takový prohřešek proti nařízení už ostatně v Česku padla i pokuta. Dostala ji banka, jejíž konkrétní název Úřad pro ochranu osobních údajů s ohledem na svá interní pravidla nezveřejnil. Sankce dosáhla 250 tisíc korun.

Z celkového počtu osmi pokut, které od účinnosti GDPR úřad udělil, je tato nejvyšší. Ostatní uložené sankce se pohybují jen v řádu desítek tisíc, ta nejnižší činí dokonce jen 5 tisíc korun. Za zveřejnění seznamu s osobními údaji na internetu tak například dostala jedna nezisková organizace sankci 10 tisíc korun. Půjčovna aut, která monitorovala vypůjčené vozy prostřednictvím GPS, pak musela zaplatit 30 tisíc korun. Z pohledu podniků jde o *„drobné“*, které bez problémů zaplatí.

O sporném přístupu firem a institucí k ochraně soukromí svědčí i opakování chyb, které odporovaly už starému českému zákonu o ochraně osobních údajů. Úřad pro ochranu osobních údajů také upozorňuje na to, že řada správců i po změně pravidel dál nadužívá souhlasy se zpracováním osobních dat anebo k jejich udělení občany nutí tvrzením, že bez něj jim nebudou moci poskytnout své služby. To ale nařízení zakazuje.

V některých případech naopak vedlo nepochopení GDPR až k *„přestřelení“* přijatých opatření. Z některých muzeí tak například s odvoláním na nařízení zmizely návštěvní knihy. V jedné pražské mateřské škole dostali rodiče pokyn, aby do omluvného listu nezapisovali děti jménem, ale vyplňovali jen značku dítěte. Místo Jana Nováka se tak omlouvá prasátko nebo chobotnička. Jinde z nástěnek sundali obrázky dětí.

Nic takového přitom evropská pravidla nenařizují. Vedení návštěvní knihy ani není zpracováním osobních údajů a podobné je to s vyvěšováním výtvarných děl. *„Tam půjde o oblast osobních práv, která je upravena v občanském zákoníku,“* říká advokát Squire Patton Boggs Jaroslav Tajbr. Místo plošného sundávání dětských výtvorů by podle něj stačilo, kdyby školy z chodeb a tříd odstranily jen obrázky a výrobky těch dětí, jejichž rodiče o to školu výslovně požádají. Omlouvání dětí je možné jednoduše řešit předáním omluvenky učitelce.

Nicméně až poněkud absurdní aplikace evropských pravidel je ve školství či jiných státních institucích snadno pochopitelná. *„Školství je dlouhodobě zatěžováno výkaznictvím, metodologiemi a jinou administrativou. Evropské nařízení tak mohlo v řadě ředitelů snadno vzbudit pocit, že je třeba papírů vyprodukovat ještě o trochu více,“* míní Tajbr. Dalším důvodem absurdních opatření pak může být to, že se školy většinou připravovaly na nařízení vlastními silami. V rozpočtech se jim podle Asociace ředitelů základních škol ČR nedostávalo peněz, aby si zaplatily konzultace s právníky.

Nepochopení mohl přinést i samotný základní koncept nařízení, který se zásadně liší od toho, co v Česku platilo dříve. *„GDPR tu není od toho, aby buzerovalo ředitelky mateřských škol nebo starosty malých obcí. Takto vnímám starý zákon o ochraně osobních údajů, který příliš nerozlišoval a vyvolával dojem, že dopadá plošně na všechny správce osobních dat,“* říká ředitel správní sekce Úřadu pro ochranu osobních údajů Josef Prokeš. Smysl nového nařízení je jiný. *„Cílí především na velká riziková zpracování osobních údajů a na dodržování pravidel ochrany soukromí při využití nových technologií,“* zdůrazňuje Prokeš.

GDPR tu není od toho, aby buzerovalo ředitelky mateřských škol nebo starosty malých obcí, připomíná Josef Prokeš z Úřadu pro ochranu osobních údajů. Nařízení cílí především na velká riziková zpracování osobních dat a nové technologie.

V očích veřejnosti

Nejsou to ale jen správci a zpracovatelé osobních údajů, kteří novým pravidlům zatím tak úplně nepřivykli. Ani občané se zatím v českých podmínkách nenaučili svá práva na ochranu osobních dat naplno využívat. Nařízení sice zvedlo vlnu zájmu o ochranu soukromí, ta ovšem záhy rychle opadla. *„V databázi spotřebitelských soutěží máme asi sto tisíc klientů, kteří nám dali souhlas se zpracováním svých údajů. Loni 25. května jsme dostali čtyři žádosti o výmaz z databáze, od té doby nic,“* popisuje například podnikový právník Coca-Coly Jan Kubíček. A podobné zkušenosti mají i další společnosti. Hlásí většinou jen jednotky žádostí o výmaz osobních údajů za celý rok a například Ekospol nebo eReading.cz dokonce uvedly, že u nich o to ještě nepožádal nikdo.

Naopak lidé mnohdy chtějí dávat souhlas i tam, kde není třeba. *„Někteří zákazníci se domnívají, že nám jej musí udělit, abychom mohli předat objednané zboží dopravci, který je bude zákazníkovi doručovat,“* popisuje typický příklad omylu advokát e-shopu Alza.cz Pavel Steinwich. V tomto případě jde ale o předání dat z titulu plnění smlouvy mezi e-shopem a jeho zákazníkem. Souhlas zákazníka tak k němu není třeba.

A další příklad rozšířeného mýtu: lidé také čekali, že je od loňského 25. května přestanou plošně obtěžovat marketingové telefonáty a e-mailové schránky jim přestanou zaplňovat spamy. Nic takového se ovšem nestalo. Jednak proto, že spíše než GDPR má problematiku nevyžádané pošty řešit jeho sesterské nařízení ePrivacy, které ale ještě Evropská unie nestihla schválit, a navíc ani GDPR nefunguje ve vakuu. Navazují na něj další zákony. *„Zákon o některých službách informační společnosti říká, že marketingová sdělení může společnost zasílat bez souhlasu svému zákazníkovi, se kterým vede jednání o smlouvě nebo s ním dříve komunikovala o nějaké transakci týkající se*

Za loňský rok podle Soni Matochové Úřad pro ochranu osobních údajů obdržel 4161 dotazů a žádostí o konzultace. Téměř polovina z nich se týkala kamerových systémů.

typově podobného zboží," vysvětluje partner advokátní kanceláře Rowan Legal Michal Nulíček.

Této výjimky hojně využívají e-shopy nebo také banky – mimo jiné ČSOB. *„Klienti, kteří se k žádosti o souhlas se zpracováním osobních údajů nevyjádřili, dostávají základní marketingovou nabídku,"* uvádí Margit Doležalová, která pracuje jako pověřenkyně pro ochranu osobních údajů v ČSOB. Od marketingových kampaní cílících na zákazníky, kteří bance souhlas udělili, se obecná nabídka liší v tom, že se neopírá o analýzu informací o konkrétním zákazníkovi. Může se tak stát, že takovému klientovi banka nabídne produkt, který už u ní má. Firmy také mohou bez souhlasu posílat zákazníkům informace technického charakteru, například avíza na plánované odstávky aplikací nebo informace o chystaném uzavření prodejen.

Správci a zpracovatelé osobních údajů rovněž mohou využívat souhlasy klientů, které získali už před účinností GDPR, pokud jejich podoba nařízení neodporuje. ČSOB tak například musela znovu žádat o souhlas se zpracováním osobních údajů k marketingovým účelům jen ty klienty, od nichž měla souhlas starší než z roku 2014.

Jak banky, tak korporace z výrobního i on-line sektoru zároveň uvádí, že se jim daří souhlasy se zpracováním osobních údajů získávat poměrně hladce. Například České spořitelně ho udělily dvě třetiny klientů, ČSOB dokonce 75 procent. Více než těch, kteří souhlas neudělili, je spíše těch, kteří se k žádosti nijak nevyjádřili. Třeba v České spořitelně se nevyjádřilo zhruba 30 procent klientů, úplných odmítnutí jsou ale jen čtyři procenta.

Internetovému obchodu Alza.cz se osvědčila taktika, že souhlas prezentuje zákazníkům jako výhodu. Jak to v praxi dělá, vysvětluje marketingový ředitel e-shopu Jan Sadílek na příkladu souhlasu s ověřením bonity zákazníka v externích databázích dlužníků při nákupu s odloženou splatností. *„Díky udělení souhlasu zákazník může dokončit objednávku o poznání rychleji, než kdybychom si bonitu ověřovali jako v minulém století tak, že by zákazník přinesl relevantní dokumenty a ty by poté posuzoval finančník,"* uvádí. Tato strategie se Alze vyplatila. Souhlasy má dle Sadílka všude, kde je potřebuje.

Práce, která nekončí

Podle odhadů Hospodářské komory stála české podnikatele adaptace na evropská pravidla zhruba 25 miliard korun. Svaz průmyslu a dopravy, který do svých propočtů zahrnul nejen podniky, ale i živnostníky, počítá celkové náklady dokonce ve stovkách miliard korun. U jednotlivých společností náklady oscilovaly od nízkých jednotek milionů korun ve výrobních podnicích, jako je Coca-Cola, až po stovky milionů korun v korporacích, pro něž je zpracování osobních údajů každodenní nutností. Česká spořitelna tak například náklady spojené s přechodem na nařízení vyčíslila na 100 milionů korun.

Tím ale výdaje na ochranu dat zdaleka nekončí. *„Není to tak, že jednou zavedu či upravím systém a již nemusím nic dělat. GDPR je proces, který by se měl stále vyhodnocovat, měla by se kontrolovat nastavená opatření,"* připomíná nejen byznysu právní expertka Hospodářské komory Lucie Plachá.

Alžběta Vejvodová
alzbeta.vejvodova@economia.cz