Adaptační zákon k GDPR byl konečně přijat

Poslanecká sněmovna dne 12. 3. 2019 schválila zákon o zpracování osobních údajů (dále jen „Adaptační zákon“) ve znění, v jakém jí byl vrácen Senátem[1], který je tzv. adaptačním zákonem k Nařízení Evropského parlamentu a Rady (EU) č. 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 (dále jen „GDPR“).

Současně pak byl schválen i doprovodný zákon k zákonu o zpracování osobních údajů (dále jen „**Doprovodný zákon**“), který byl schválen ve verzi přijaté již dříve Poslaneckou sněmovnou[2].

Zákony nabydou účinnosti v nejbližších dnech, a to vyhlášením ve Sbírce zákonů. Shrnuli jsme pro Vás to nejdůležitější, co nové právní předpisy přináší a znamenají.

Adaptační zákon

Většina ustanovení Adaptačního zákona upřesňuje či rozvádí již zavedená ustanovení GDPR. Zákonodárce ale využil i možnosti odchýlit se od úpravy GDPR a stanovuje určité výjimky. Zákon například stanovuje hranici pro **způsobilost dítěte k udělení souhlasu se zpracováním osobních údajů** v souvislosti s nabídkou služeb informační společnosti (např. zpracování osobních údajů provozovateli sociálních sítí) na 15 let. Český zákonodárce tak hranici stanovenou GDPR snížil o jeden rok.

Další z výjimek, které Adaptační zákon přináší je například **omezení povinnosti správce osobních údajů vypracovat posouzení vlivu zpracování osobních údajů (DPIA)** v situaci, kdy mu provedení takového zpracování osobních údajů stanovuje přímo právní předpis.

S uvedeným souvisí i možnost správce osobních údajů splnit svou informační povinnost vůči subjektům údajů **zveřejněním způsobem umožňujícím dálkový přístup**, a to v případě, kdy osobní údaje zpracovává na základě zákonné povinnosti či ve veřejném zájmu. Typicky tak půjde například o plnění informační povinnosti zaměstnavatele vůči zaměstnancům, kdy nebude potřeba, v souladu se zněním nového zákona, nezbytné, aby byl každý zaměstnanec informován samostatně.

V Adaptačním zákoně je také více detailněji upraveno zpracování osobních údajů pro účely **vědeckého nebo historického výzkumu či pro statistické účely**. Stejně tak se zákon podrobněji věnuje zpracování osobních údajů pro novinářské účely či pro účely **akademického, uměleckého nebo literárního projevu**. V těchto případech zákon omezuje právo subjektu údajů na přístup k osobním údajům dle GDPR, a to s ohledem na ochranu zdroje a obsahu informací. Zákon tak do jisté míry vyjasňuje situace, kdy jsou novináři, umělci apod. povinni sdělovat subjektům údajů informace ohledně zpracování jejich osobních údajů.

Adaptační zákon dále stanovuje určité výjimky například pro **povinnost posuzování slučitelnosti účelů, povinnost oznámení porušení zabezpečení osobních údajů subjektu údajů či uplatnění některých dalších práv a povinností**.

Významná část Adaptačního zákona je pak věnována **ochraně osobních údajů při jejich zpracování za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti a ochraně osobních údajů při zajišťování obranných a bezpečnostních zájmů České republiky**.

Oproti původnímu návrhu Poslanecké sněmovny a na základě pozměňovacích návrhů Senátu došlo k úplnému **vypuštění pravomocí Úřadu pro ochranu osobních údajů v oblasti svobodnému přístupu k informacím**.

V neposlední řadě je nutné podotknout, že nabytím účinnosti nového zákona se mj. zrušuje dosavadní zákon č. 101/2000 Sb., o ochraně osobních údajů, ve znění pozdějších předpisů, a nový zákon společně s GDPR jej tak zcela nahrazují.

Přestupky a sankce

GDPR umožňuje členským státům samostatně upravit pravidla ukládání správních pokut orgánům veřejné moci a veřejným subjektům. Český zákonodárce při přípravě nového Adaptačního zákona této možnosti využil a v Adaptačním zákoně stanovil, že s výjimkou následujícího odstavce orgánům veřejné moci a veřejným subjektům usazeným v České republice, ač by se dopustili porušení některé povinností podle GDPR nebo Adaptačního zákona, nebude správní trest (pokuta) uložen (resp. bude od uložení upuštěno).

Adaptační zákon dále omezuje výši pokuty, která může být v souvislosti s porušením některých povinností v souvislosti s ochranou osobních údajů právnickou osobou, zejména ve vztahu při zpracování osobních údajů za účelem předcházení, vyhledávání nebo odhalování trestné činnosti, stíhání trestných činů, výkonu trestů a ochranných opatření, zajišťování bezpečnosti České republiky nebo zajišťování veřejného pořádku a vnitřní bezpečnosti, na 10.000.000,- Kč.

Za přestupek spočívající v porušení zákazu zveřejnění osobních údajů stanoveného jiným právním předpisem lze uložit pokutu do 1.000.000,- Kč, nebo 5.000.000,- Kč, půjde-li o přestupek spáchaný tiskem, filmem, rozhlasem, televizí, veřejně přístupnou počítačovou sítí nebo jiným obdobně účinným způsobem.

Adaptační zákon přináší také některé další nové přestupky, a to nad rámec přestupků v GDPR související s porušením povinností, které stanovuje přímo tento zákon. S těmito přestupky jsou spojeny také samostatné sankce. Výše uvedené upuštění od sankce pro orgány veřejné moci a veřejné subjekty se však uplatní i zde.

Projednání přestupků a vybírání pokut dle tohoto zákona má ve své pravomoci dozorový úřad, jímž je v tomto případě Úřad pro ochranu osobních údajů (ÚOOÚ). Zákonodárce však umožňuje ÚOOÚ uložit správci či zpracovateli, který povinnosti stanovené zákonem či GDPR porušil, opatření k odstranění zjištěných nedostatků a stanovit lhůtu pro jejich odstranění. V takových případech pak v souladu se zákonem může ÚOOÚ od uložení správního trestu upustit.

Doprovodný zákon

Doprovodný zákon mění **některé další zákony v souvislosti s přijetím Adaptačního zákona**, když zejména upravuje zpracování osobních údajů pro účely plnění úkolů ve veřejném zájmu a řeší i vybraná specifika zpracování osobních údajů ze strany jednotlivých složek veřejné správy.

Závěr

Nově přijaté právní předpisy **dokončují proces první vlny adaptace právního řádu České republiky na GDPR**. V budoucnu lze očekávat další změny právní úpravy, zejména ve vztahu k některým službám informační společnosti a e-commerce (obchodní sdělení, cookies) a pracovnímu právu.

Zákony nyní poskytují dostatečný právní rámec pro ÚOOÚ, aby mohl efektivně vykonávat svoji dozorovou a kontrolní činnost v oblasti ochrany osobních údajů, která byla od data použitelnosti GDPR poněkud oslabena s ohledem na chybějící adaptační právní úpravu.

Autoři: Mgr. Barbora Cetkovská, Mgr. Jakub Málek (PEYTON legal)

(www.epravo.cz 3. 4. 2019)

Život s GDPR – blíží se výročí

Příliš mnoho nechybí a budeme za sebou mít první rok soužití s GDPR. Mnoho laiků i odborníků vnímá celou problematiku jako zbytečně nafouklou a zbytečně dramatizovanou. Pojďme se podívat, jak se naplnila očekávání, a hlavně jaký vývoj nás v této oblasti ještě může potkat. Na úvod si pojďme říct několik zajímavých čísel.

GDPR v několika číslech

Abychom si mohli utvořit představu, jak se nová pravidla pro ochranu osobních údajů, a především jejich vymáhání, projevila v praxi, stačí se podívat na počet podnětů (udání), které obdržel Úřad pro ochranu osobních údajů v loňském roce. Samozřejmě část z nich spadá i do období před účinností nařízení, nicméně po datu účinnosti lze sledovat razantní navýšení podnětů. Úřad obdržel celkem 3616 podnětů, z toho jen 260 se týkalo porušení bezpečnosti údajů a 2901 směřovalo na problematiku nevyžádaných obchodních sdělení, kterými se ve smyslu zákona 480/2004 Sb., o některých službách informační společnosti, úřad také musí zabývat. Vzhledem k omezeným lidským zdrojům dozorového úřadu bylo zahájeno 76 nových kontrol na dodržování pravidel ochrany osobních údajů a dalších 22 na problematiku nevyžádaných obchodních sdělení. Tato čísla uvádím pouze pro ilustraci toho, jak subjekty údajů naložili s možností stěžovat si, případně si i v rámci podnikání vyřizovat účty s konkurencí. Současně tato čísla také ukazují na možnosti a kapacity dozorového úřadu, a tedy i na pravděpodobnost namátkové kontroly. Úřad v rámci své kontrolní činnosti, a v souladu s kontrolním plánem, provádí i kontroly, které nejsou založené na podnětu, nicméně jejich množství je značně omezené.

Zcela bez diskuze příprava na GDPR znamenala velké množství práce pro poradce, nejen z řad advokátů a IT odborníků. Kromě úvodní vlny, kdy si řada subjektů nechala vypracovat úvodní analýzu za desítky až stovky tisíc korun, představuje GDPR i trvalý zdroj příjmu pro pověřence pro ochranu osobních údajů. Někteří pověřenci plní tuto funkci až pro 203 subjektů současně, což vzhledem k tomu, že jedním z parametrů na výkon funkce pověřence je „snadná dostupnost“ pro správce i subjekty údajů, jejichž údaje správce zpracovává, lze považovat za nadlidský výkon. Potřebnost této pozice nebo služby zůstává i po téměř roce účinnost dle mého názoru velice sporná, když podle dozorového úřadu více než 40 % po-

věřenců nebylo od loňského května ze strany správce osobních údajů vůbec kontaktováno a jejich služby tedy nebyly zatím potřeba.

Promítnutí GDPR do národní legislativy

V rámci Evropské Unie přijalo prováděcí předpisy k GDPR 23 států, pouze 4 státy to dosud nezvládly – Česká republika se ze seznamu opozdilců nakonec dostala teprve minulý měsíc, když se podařilo schválit návrh nového zákona o ochraně osobních údajů „již" v první polovině března 2019.

Prodleva mezi účinností nařízení a přijetím nového zákona o ochraně osobních údajů sehrála určitou roli v nedostatečné právní jistotě těch, na které norma dopadá. Toto se kromě komerčních subjektů dotklo i veřejnoprávních subjektů, které musely ze svých omezených rozpočtů nemálo investovat na zavedení opatření k zajištění souladu s novými pravidly. Časem se ukázalo, že není příliš jasné, co mají vlastně některé organizace pro dosažení souladu s GDPR vlastně udělat. Můžeme se tak dodnes setkat s řadou institucí, které jmenovaly svého pověřence pro ochranu osobních údajů, ale dle nařízení ho mít nemusejí, například muzea, knihovny, divadla nebo některé další příspěvkové organizace.

Domnívám se, že tato nejistota způsobená absencí nového zákona o ochraně osobních údajů, který by v některých bodech zmírnil dopady GDPR, se projevila i v závěrech z provedených kontrol ze strany Úřadu pro ochranu osobních údajů. I přes vysoké finanční limity pokut, často likvidačního charakteru, které GDPR stanovuje a umožňuje dozorovým úřadům v členských státech ukládat, uložil Úřad v řadě provedených kontrol pouhé napomenutí nebo nápravné opatření a pouze v ojedinělých případech sáhnul k samotnému uložení pokuty. Tyto pokuty nebyly dle mého názorů ani vysoké či likvidační a v případě, že kontrolovaný správce údajů poskytoval součinnost, bylo evidentní, že se Úřad spíše snaží pomoci a vyjasnit některé nepřesnosti, ke kterým při překotném zavádění nových opatření docházelo. Nabízí se nyní otázka, zda bude tento vstřícný přístup pokračovat i dále, kdy už od účinnosti GDPR uplynul téměř rok a kdy i Česká republika bude mít konečně zákon o ochraně osobních údajů reflektující GDPR. Po seznámení se s konečným zněním nového zákona můžete nicméně nabýt dojmu, že zákonodárci celkem úspěšně obešli některé principy GDPR.

Nový zákon – vyjasnění nejasností a obav

Účinnost nového zákona nebude znamenat v podstatě žádné zásadní změny ve fungování oproti dosavadnímu stavu po účinnosti GDPR, všichni budou muset alespoň projít své vnitřní předpisy k GDPR a nahradit odkazy na zákon 101/2000 Sb. odkazy na zákon nový.

Drobnou změnou nebo vyjasněním je stanovení věkového limitu způsobilosti dítěte udělovat souhlas se zpracováním osobních údajů od patnácti let, kdy nařízení umožňovalo členským státům zvolit tento limit v rozmezí již od třinácti let věku dítěte. Důležité je si uvědomit, že takto udělený souhlas bude platný pouze v případě jeho souvislosti s nabídkou služeb informační společnosti přímo dítěti. Na jiné typy souhlasů se zpracováním údajů se tento věkový limit neuplatní.

Příjemnou úlevou z administrativních povinností je výjimka z povinnosti provádět posouzení vlivu zpracování osobních údajů na ochranu osobních údajů, kdy takové posouzení není třeba provádět v případě, že právní předpis stanoví povinnost takové zpracování osobních údajů provést. Zdá se to jako zcela logické, nicméně ne všechny povinnosti kladené na správce údajů v původním textu nařízení logické jsou a často mohou působit jako přehnaná administrativa.

I přes některé obavy českých médií a přehnaně prezentované nebezpečí pro svobodu slova, nový zákon o ochraně osobních údajů jasně stanovuje pravidla pro zpracování osobních údajů pro novinářské účely nebo pro účely akademického, uměleckého nebo literárního projevu, kdy při dodržení základních pravidel a určité míry proporcionality užití a oprávněných zájmů dotčených subjektů údajů není zpracování osobních údajů jakkoli nestandardně omezeno. Stejně tak je zachována i ochrana zdroje informací v rámci svobodné žurnalistiky.

Limity pro ukládání pokut

Pro řadu subjektů bude nový zákon o ochraně osobních údajů představovat v podstatě čistě formální změny v textaci vnitřních předpisů. Celkově dochází k určitému uklidnění, kdy nový zákon potvrzuje maximální výši pokut na hranici deseti milionů korun, se kterou pracoval i předchozí zákon o ochraně osobních údajů č. 101/2000 Sb. Pro veřejnoprávní organizace bude nová zákonná úprava znamenat zásadní úlevu, kdy nový zákon zcela zásadním způsobem limituje výši pokut, které lze za porušení pravidel ochrany osobních údajů uložit. Za porušení zákazu zveřejnění osobních údajů tak podle nové úpravy hrozí obcím, které nevykonávají přenesenou působnost v rozsahu obecního úřadu obce s rozšířenou působností, dobrovolným svazkům takových obcí, příspěvkovým organizacím zřizovaným takovou obcí nebo právnickým osobám vykonávajícím činnost školy nebo školského zařízení pokuta nejvýše 5.000 Kč a v případě, že se přestupku dopustí tiskem, filmem, rozhlasem, televizí, či veřejně přístupnou počítačovou sítí, nejvýše 15.000 Kč.

Za řadu dalších přestupků hrozí veřejnoprávním organizacím pokuta do výše 5.000 Kč a jen ve výjimečných případech týkajících se porušení systémového charakteru může dojít k uložení pokuty přesahující tuto hranici. Zákonodárce měl v tomto případě možnost finančního postihu veřejnoprávních organizací vynechat úplně, nicméně na tomto bodu se neshodla

poslanecká sněmovna se senátem a díky tomuto bodu se návrh zákona vracel ze senátu zpět do sněmovny a celý legislativní proces se tím prodloužil.

Nicméně i bez hrozby likvidačních sankcí by správci údajů měli dbát dodržování pravidel zpracování osobních údajů, a to nejen kvůli zákonu, ale i kvůli reputačnímu riziku, které je s případným porušením a únikem údajů spojeno.

Závěr

Sjednocení a modernizace přístupu k ochraně osobních údajů v dnešní době informační společnosti je zcela nezbytná. Všechna opatření k zajištění souladu je ale nutné dělat částečně s využitím selského rozumu, přiměřeně zpracovávaným údajům a okolnostem každého správce údajů. I pokud se nad námi nehoupe meč v podobě hrozby pokuty do 20 milionů eur, není radno ochranu údajů zanedbat. A jak se ukazuje v řadě evropských států, především společnosti podnikající v digitálním prostoru by měly brát ochranu údajů vážně. Jako příklad za všechny lze uvést nedávné postihy pro Facebook a Google v západní Evropě.

Autor: Mgr. Radomír Pivoda (AK Pavelka)

(www.epravo.cz 15. 4. 2019)

GDPR v praxi. Aneb Téměř rok zkušeností napříč regionem

Evropské nařízení o ochraně osobních údajů vyvolalo celosvětový rozruch. Ovšem i přes velkou pozornost, které se mu dostalo, v praxi stále přetrvává řada výkladových nejasností.

V květnu tomu bude rok, co se evropská společnost více či méně ochotně přizpůsobila nařízení o ochraně osobních údajů, anglicky General Data Protection Regulation (GDPR).[1] Ačkoliv toto nařízení ve většině případů pouze navázalo na dosavadní evropská pravidla pro ochranu osobních údajů, některé nové povinnosti a přísnější sankce vyvolaly bez nadsázky celosvětový rozruch.

Důvodem je v první řadě široká působnost nařízení. Vztahuje se totiž i na subjekty mimo Evropskou unii za předpokladu, že v EU působí nebo zpracovávají údaje občanů členských států. Totéž platí i pro ustanovení upravující výše sankcí za porušení. Dnem účinnosti nařízení tak například přestaly být pro Evropany dočasně dostupné některé americké webové stránky, a v Austrálii se dokonce začalo debatovat, zda by i tam nemělo dojít k rozšíření ochrany osobních údajů po vzoru GDPR.

V evropských zemích pak po celý minulý rok probíhala informační smršť. Pořádalo se nesčetně školení, publikovalo tisíce článků a e-mailové schránky nás všech se plnily žádostmi o udělení nových souhlasů.

Celá oblast ochrany osobních údajů i profese, které se jí věnují, zažily nevídaný rozmach. I přes tuto pozornost, které se nařízení dostalo, však v praxi stále přetrvává řada výkladových nejasností. V tomto článku přinášíme jedinečné shrnutí zkušeností a postřehů právních poradců Deloitte Legal nejen v České republice, ale také z Pobaltí či regionu středovýchodní Evropy, které Deloitte Legal již dříve vydal formou reportu pod názvem The GDPR: Six Months After Implementation.[2]

Úskalí dobrovolnosti

Jedním z nejčastějších problémů je přílišné nadužívání souhlasů ke zpracování osobních údajů. Příčinou tohoto problému je pravděpodobně nepochopení základních konceptů GDPR. Pokud existuje jiný právní důvod pro zpracování osobních údajů, jako například plnění smlouvy, oprávněný zájem správce nebo zákonná povinnost, není vyžádání souhlasu tím správným postupem.

Podmiňuje-li navíc obchodník poskytnutí služby či zboží udělením souhlasu k takovému zpracování osobních údajů, které jinak není pro poskytnutí dané služby nebo zboží nutné, svědčí to o tom, že souhlas nebyl udělen dobrovolně. Jenže podmínku dobrovolnosti právě nařízení vyžaduje.

---

[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).

[2] Celé znění dostupné na stránkách www.deloitte.com. Nadužívání souhlasů uvádí i český Úřad pro ochranu osobních údajů jako jeden z deseti nejčastějších omylů při výkladu GDPR. Zároveň je tento problém ukázkou toho, že určité výkladové nejasnosti existovaly i před účinností nařízení.

Každý má přitom právo udělený souhlas odvolat. Pokud o to dotyčný požádá, musí být správce schopen rozlišit, jaké údaje zpracovával na základě ostatních právních důvodů a jaké na základě souhlasu. Následně by měl svého zákazníka či klienta informovat o tom, jaké údaje bude i nadále zpracovávat. Například odvolání souhlasu k zasílání nejrůznějších informací nezbavuje správce povinnosti dodávat zboží podle smlouvy, a to bez zpracování některých údajů nejde.

Pokud také správce informuje subjekt, že údaje zpracovává na základě souhlasu, ačkoliv mu taková povinnost už plyne ze zákona, neplní řádně svou informační povinnost.

Nadužívání souhlasů uvádí i český Úřad pro ochranu osobních údajů jako jeden z deseti nejčasnějších omylů při výkladu GDPR.[3] Zároveň je tento problém ukázkou toho, že určité výkladové nejasnosti existovaly i před účinností nařízení. Nadužíváním souhlasů se totiž úřad zabýval i před platností nařízení.[4]

Společnosti také často bojují s vymezením pojmů jako „správce“, „společný správce“ a „zpracovatel“. Řada správců se na zpracovatele snaží přenést nadmíru povinností a ti tak raději usilují o to, aby byli rovnou považováni za samostatné správce. Například bulharský úřad v tomto ohledu vydal stanovisko, že banky, pojišťovny a přepravní společnosti by měly být považovány za správce, jelikož často poskytují přísně regulované služby na základě licence získané od státu. Obdobná stanoviska vydávají i v českém prostředí komory či sdružení společností vykonávajících regulovanou činnost.

Dalším problémem je nedostatečná vzdělanost a přehled o základních principech ochrany osobních údajů. Správcům se často stává, že pravidla, jimiž se zpracování má řídit, jsou roztříštěna v několika dokumentech, což způsobuje nedostatek transparentnosti. Absence vhodných technologických řešení brání zase tomu, aby byla dodržována pravidla pro minimalizaci údajů, výmaz dat a dodržování doby uchovávání. Problém v praxi představuje i samotné vymezení přípustné doby uchování. V některých státech, jako třeba v Rumunsku či Maďarsku, se navíc potýkají s nedostatkem výkladových stanovisek a jiných forem šíření osvěty ze strany dozorových úřadů.

Jak zapojit zaměstnance

V praxi se zejména větším společnostem nejlépe osvědčil komplexní přístup k problematice GDPR, který zahrnuje a sjednocuje právní, informačně-technologické i obchodní aspekty. Progresivní jsou řešení, která se neomezují jen na splnění minimálních požadavků, ale zavádí moderní systémy, jež umožňují i vyhodnocování rizik a jiné funkcionality.

Jak se zdá, nejefektivnější je nejen zaměstnance školit, ale také je přímo zapojit do implementace nových pravidel v rámci jejich každodenních pracovních úkonů. Většina společností aktualizovala dokumentaci související se zpracováním osobních údajů nebo si vyžádaly souhlasy v nové podobě. Řada podnikatelů na svých stránkách zveřejnila jednotný formulář pro jednotlivé požadavky vznesené subjekty údajů. To jim umožňuje tyto podněty zpracovávat ve standardizované podobě a šetřit čas. Zaměstnavatelé také umisťují na webové stránky informace o zpracování osobních údajů pro uchazeče o práci či pro své zaměstnance vypracovávají interní pravidla.

Osvěta přechází v kontrolu

V souvislosti se zavedením GDPR národní úřady zaznamenaly značný nárůst stížností. Úřady jednotlivých zemí se dlouhou dobu zaměřovaly především na vzdělávání veřejnosti, ovšem jejich pozornost se čím dál více upírá i na kontrolní činnost a v Polsku už nedávno dokonce padla i první větší pokuta ve výši 220 tisíc eur. Ostatně řada zemí plánuje významné rozpočtové, potažmo personální posílení příslušných institucí.

Tuzemský Úřad pro ochranu osobních údajů už avizoval, že kontroly budou zaměřeny spíše na celkové pochopení nároků GDPR a řešení odpovědnosti společností nežli na nedostatky v jednotlivých procesech zpracování.

Na osvětovou činnost úřadů pak navazuje řada zájmových a profesních organizací ve formě vydávání kodexů chování podle článku 40 nařízení, vzorových dokumentů a průvodců nebo odpovědí na nejčastější otázky. V České republice jsou v této oblasti aktivní například Asociace pro elektronickou komerci, Asociace malých a středních podniků a živnostníků ČR, Česká advokátní komora, Komora auditorů ČR nebo Česká lékařská komora a některá ministerstva.

Většina předmětných států již přijala předpisy, které reflektují GDPR. Některé země se rozhodly pouze doplnit a upřesnit pravidla nastolená nařízením, jinde – jako například na Slovensku – zákonodárci přijali komplexní zákon zrcadlící systém GDPR. V Polsku v souvislosti se změnou legislativy došlo i k přesunu kompetencí na jiný orgán a k vytvoření nových poradních orgánů. Těmto orgánům také přibylo do kompetence schvalování kodexů chování.

Nejčastější národní odchylkou od GDPR je stanovení přísnějších pravidel pro zpracování rodných čísel nebo jejich ekvivalentů a údajů o zaměstnancích. V Lotyšsku také byla stanovena promlčecí doba pro uplatnění nároků z nezákonného zpracování (pět let od spáchání nebo od ukončení protiprávního stavu, pokud stav trval déle) a výjimky pro novinářské,

[3] Desatero omylů. Dostupné na stránkách Úřadu pro ochranu osobních údajů.

[4] Stanovisko č. 3/2014 K nadbytečnému vyžadování souhlasu se zpracováním osobních údajů a souvisejícímu nesprávnému plnění informační povinnosti. Dostupné na stránkách Úřadu pro ochranu osobních údajů. Zejména větším společnostem se osvědčil komplexní přístup k problematice GDPR, který zahrnuje a sjednocuje právní, informačně-technologické i obchodní aspekty. Progresivní jsou řešení, která se neomezují jen na splnění minimálních požadavků.

vzdělávací nebo umělecké účely. V České republice prozatím formálně zůstává účinný zákon o ochraně osobních údajů, avšak ustanovení GDPR mají před ním přednost. Nový zákon by měl vejít v účinnost v nejbližších dnech, avšak pro soukromý sektor by neměl oproti původnímu nařízení představovat žádnou zásadnější odchylku.

GDPR jako příležitost

Jak již bylo zmíněno v úvodu, ve všech analyzovaných zemích byl v loňském roce zaznamenán masivní nárůst požadavků o znovuudělení souhlasu ke zpracování osobních údajů nebo k udělení souhlasu v novém znění. Hojně se také zasílaly nové informace o zásadách zpracování osobních údajů. Podle jednotlivých odvětví a vztahu správce k subjektu údajů byly souhlasy vyžadovány buďto rovnou, nebo postupně prostřednictvím budoucí komunikace s klienty. Nejčastější formou byl email, ale využívaly se i webové stránky, SMS, telefonické hovory, nebo klasické dopisy. Vyžadování nového souhlasu nebylo nutné, pokud způsob udělení původního souhlasu za předešlé úpravy byl v souladu s podmínkami GDPR.[5]

Jelikož GDPR je stále relativně novým předpisem, jehož míra obecnosti je obrovská a šíře působnosti enormní, budou problémy spojené s jeho výkladem a aplikací přetrvávat i v nejbližší budoucnosti. Pochopením základních principů evropského pojetí ochrany osobních údajů a šířením osvěty však lze předcházet těm nejrozšířenějším omylům, jako je například nadužívání souhlasů.

Velkou výzvu představuje pro správce a zpracovatele nejen jednorázové přizpůsobení se GDPR, ale především průběžné plnění jeho požadavků a zajištění průběžného souladu. To je podle našeho názoru úkol, kterým se nyní bude zabývat značná část odborníků v oblasti ochrany osobních údajů, ale také technologií a compliance obecně.

Podle našich dosavadních zkušeností mají společnosti největší rezervy v oblastech, jako jsou zpřesňování interních pokynů, vytváření srozumitelnějších metodik, zavádění opatření k vytvoření efektivního compliance programu v oblasti ochrany osobních údajů a vzdělávání pověřenců či interních odborníků.

Nejvhodnějším řešením je jistě komplexní přístup k ochraně osobních údajů, který nebude nová opatření brát jen jako nutné „regulatorní zlo“, ale jako příležitost, jak lépe budovat důvěru u klientů, jak využít pořádek v datech v rámci nových byznysových příležitostí a jak se otevřít technologickému pokroku.

Jak se žije s GDPR

Obávané nařízení o ochraně osobních údajů je účinné od loňského května. Za tuto dobu došlo v Evropě celkově k téměř 60 tisícům případů porušení pravidel GDPR. Ve kterých zemích je příliš nerespektují?

O autorech: Martina Heřmanová, advokátka, Deloitte Legal, Lukáš Holub, advokátní koncipient, Deloitte Legal

[5] Důvod č. 171 GDPR.

Jak se žije s GDPR

Obávané nařízení o ochraně osobních údajů je účinné od loňského května. Za tuto dobu došlo v Evropě celkově k téměř 60 tisícům případů porušení pravidel GDPR. Ve kterých zemích je příliš nerespektují?

Počet případů porušení v období od 25. května 2018 do 28. ledna 2019

Počet porušení ochrany osobních údajů na 100 tisíc osob

Nejvýše udělené pokuty v rámci EU od 25. května 2018 do 28. ledna 2019

ZEMĚ	Výše pokuty	Případ porušení
FRANCIE	50 mil. eur	Společnost Google zpracovala osobní údaje bez platného titulu.
NĚMECKO	80 tis. eur	Nedostatečně provedené zašifrování hesel zaměstnanců, které vyústilo v únik osobních údajů.
NĚMECKO	20 tis. eur	Únik zdravotních dat pacientů.

Zdroj: DLA Piper

(Právní rádce 5. 4. 2019)

První pokuty za porušení GDPR jsou na světě

Půl roku po nabytí účinnosti GDPR (General Data Protection Regulation) byly v Portugalsku a Francii uloženy první pokuty za porušení daného nařízení. Sankcionovanými subjekty jsou poskytovatel zdravotních služeb a společnost Google LLC. Jelikož GDPR předpokládá zjednodušení postupu úřadů na ochranu osobních údajů napříč celou EU, jsou tato rozhodnutí relevantní i v českých podmínkách. Níže uvádíme pár zajímavostí a doporučení, které je možné na jejich základě vyvodit:

Rozhodnutí ve věci Google LLC

Francouzský úřad na ochranu osobních údajů uložil 21. ledna 2019 pokutu ve výši 50 miliónů EUR americkému IT gigantovi Google LLC. Dané řízení bylo zahájeno na základě podnětu sdružení zastupujícího přibližně 10.000 subjektů údajů. Vytýkané nedostatky zahrnovaly:

Nedostatečnou transparentnost a informování

Úřad konstatoval, že informační povinnost nebyla dostatečně splněna, protože informace poskytované subjektům údajů nebyly lehce přístupné. Struktura informací o zpracování osobních údajů nebyla v souladu s GDPR, jelikož podstatné informace, jako účel zpracování, doba uložení či kategorie osobních údajů zpracovávaných za účelem personalizace reklam byly nekompaktně roztroušeny v několika samostatných dokumentech. Relevantní informace byly dostupné ze strany subjektu údajů až po šestém prokliku.

Úřad také konstatoval, že některé informace nebyly vysvětleny dostatečně jasně a srozumitelně, v důsledku čehož uživatelé neměli šanci porozumět rozsahu zpracovatelských operací. Současně nebyl jasně uveden souhlas jako právní základ pro personalizaci reklam a doby uložení pro některé kategorie údajů nebyly uvedeny vůbec.

Neplatný souhlas pro personalizaci reklam

Google zpracovává osobní údaje za účelem personalizace reklam, a to na základě souhlasu. Úřad však vyslovil, že souhlasy subjektů údajů nebyly platně poskytnuty právě kvůli nedostatečnému informování subjektů údajů. Opět, předmětné informace se nacházely v několika samostatných dokumentech a průměrně zkušený uživatel služby neměl možnost porozumět tomu, že za účelem personalizace reklamy se zpracovávají jeho údaje získané a zkombinované z různých služeb (např. Google search, You tube, Google maps).

Souhlas měl být dán neplatně také proto, že byl udělen prostřednictvím dopředu označeného nástroje, a současně proto, že souhlas mohl být dán pouze souhrnně pro všechny v něm uvedené zpracovatelské operace bez možnosti vynětí některých operací. Postup tak nesplňoval požadavek, aby byl souhlas udělený pro každý účel zpracování samostatně.

Na základě výše uvedeného konstatování ze strany Úřadu je možné vyvodit kritéria pro transparentnost, efektivní informování a udělování souhlasu.

Zajímavostí však je, že řízení bylo vedeno vůči společnosti Google LLC se sídlem v USA a ne proti její evropské centrále sídlící v Irsku (v tomto případě by totiž byl pro řízení příslušný irský, a ne francouzský regulátor). Důvodem tohoto postupu bylo zjištění, že v souvislosti s aktivitami, které byly předmětem kontroly, neměla irská společnost Google žádnou rozhodovací pravomoc a za správce se tedy považovala výlučně americká mateřská společnost. V této souvislosti bude velmi zajímavé sledovat, jak se k vykonatelnosti sankce uložené evropským orgánem vůči subjektu sídlícímu mimo EU postaví dotčené subjekty. S ohledem na silné postavení společnosti Google LLC na evropském trhu bude do určité míry precedentní, jak bude v praxi fungovat ambiciózní ustanovení GDPR o jeho působnosti i mimo území EU.

Rozhodnutí ve věci poskytovatele zdravotních služeb

Prvenství v uložení finanční sankce za porušení ustanovení GDPR však patří portugalskému úřadu na ochranu osobních údajů. Sankcionovaným subjektem je poskytovatel zdravotních služeb, kterému byla uložena pokuta v celkové výši 400,000 EUR. Zjištěná porušení:

Neúčinná minimalizace údajů

Úřad konstatoval porušení zásady minimalizace údajů, která upravuje, že osobní údaje musí být přiměřené, relevantní a omezené na rozsah, který je nevyhnutelný vzhledem k účelům, pro které se zpracovávají. Tato zásada měla být porušena tím, že zdravotnické zařízení mělo umožnit přístup k údajům pacientů nadměrnému počtu uživatelů, u kterých, podle úřadu, k tomu neexistoval důvod. Za toto porušení byla uložena pokuta 150,000 EUR.

Nedostatečné zabezpečení údajů

Dále bylo zjištěno porušení zásady integrity a důvěrnosti, podle které osobní údaje musí být zpracovávány způsobem, který zaručuje přiměřené zabezpečení osobních údajů, včetně ochrany před neoprávněným anebo nezákonným zpracováváním a náhodnou ztrátou, zničením či poškozením, a to prostřednictvím přiměřených technických anebo organizačních opatření. Nemocnice měla porušit svoji povinnost zavést technická a organizační opatření na zabránění nezákonnému přístupu k údajům. Za toto porušení byla uložena pokuta ve výši 150,000 EUR.

Nakonec regulátor sankcionoval pokutou ve výši 100,000 EUR porušení povinnosti přijmout přiměřená dostatečná technická a organizační opatření s cílem zajistit úroveň zabezpečení odpovídající riziku. Úřad zjistil, že nemocnice nezabezpečila trvalou důvěrnost, integritu, dostupnost a odolnost systémů zpracování a služeb a proces pravidelného testování, posuzování a hodnocení účinnosti technických a organizačních opatření na zajištění zabezpečení zpracování.

Skutečnosti, které byly rozhodující v kontrolním procesu:

- neexistence interních směrnic správce, které by upravovaly souvislost mezi funkčním zařazením uživatele do informačního systému a rozsahem, v jakém má uživatel přístup k informacím, včetně informací o zdravotním stavu;
- neexistence dokumentu určujícího postup vytváření uživatelských účtů v informačním systému;
- techničtí zaměstnanci měli přístupová práva nastavená tak, jako kdyby byli zdravotnickými pracovníky, v důsledku čehož měli neomezený přístup ke zdravotním údajům dotčených osob;
- nastavení systému umožňovalo všem lékařům, bez ohledu na specializaci, přístup k jakýmkoliv zdravotním údajům pacienta; uvedený postup se považoval za porušení zásady, že oprávněná osoba má mít přístup jen k takovým údajům, které nevyhnutelně potřebuje pro výkon své činnosti („need-to-know basis“);
- v informačním systému bylo 985 uživatelů majících přístupové oprávnění na úrovni „lékař“, ale správce reálně zaměstnával pouze 296 lékařů;
- uživatelské účty lékařů, kteří přestali vykonávat činnost pro nemocnici, se nedeaktivovaly.

Výše uvedené poznatky můžou sloužit poskytovatelům zdravotních služeb, ale i jiným správcům jako inspirace při vytváření vnitřních postupů a směrnic týkajících se přístupu k osobním údajům a jejich zpracování.

Autor: JUDr. Helga Maďarová, CIPP/E, CIPM (Dvořák Hager & Partners)

(www.epravo.cz 27. 2. 2019)

Ochrana oznamovatelů (whistleblowerů) v České republice?

Ministerstvo spravedlnosti předložilo 18. 2. 2019 vládě k projednání návrh zákona o ochraně oznamovatelů[1]. Tématem oznamování protiprávních jednání, o kterých se oznamovatelé dozví v souvislosti se svým zaměstnáním (známé také pod anglickým pojmem „whistleblowing“), se zákonodárce zabýval opakovaně. Žádná komplexní úprava, která by toto téma řešila a která by podpořila oznamovatele a poskytla jim náležitou ochranu, však dosud přijata nebyla.

V současné době je ochrana oznamovatelů řešena i v rámci Evropské unie, kdy od první poloviny loňského roku je v Evropském parlamentu a Radě projednáván návrh Směrnice o ochraně osob oznamujících porušení práva Unie[2].

Cíle návrhu

Cílem návrhu českého zákona je zajistit zaměstnancům, státním zaměstnancům ve služebním poměru, vojákům z povolání nebo členům bezpečnostních sborů (v tomto článku pro zjednodušení dále jen souhrnně jako „zaměstnanci“) vhodné prostředí a důvěryhodné kanály pro oznámení protiprávních jednání, o kterých se dozvěděli v souvislosti se svým zaměstnáním či službou. Protiprávním jednáním se pro účely návrhu zákona rozumí trestný čin, přestupek a jednání, které má znaky trestného činu nebo přestupku.

Jak jsme již naznačili výše, v současné chvíli není ochrana oznamovatelů v českém právním řádě souhrnně zakotvena a je tak dovozována z obecných institutů jednotlivých předpisů trestního či správního práva, a především pak z práva pracovního a dalších předpisů, na jejichž základě je založen příslušný vztah mezi zaměstnavateli a zaměstnanci. Výjimkou jsou oznamovatelé z řad státních zaměstnanců, kteří jsou již nyní výslovně chráněni proti negativním dopadům oznámení na

[1] Návrh zákona je k dispozici zde.
[2] Návrh směrnice je k dispozici zde.