- Jaké změny nás čekají v právní úpravě pro oblast kybernetické bezpečnosti
- Dodatečné daňové přiznání vs. daňová kontrola: Jak mají společnosti postupovat, pokud se u nich plánuje daňová kontrola?
- Návrh zákona o centrální evidenci účtů schválen vládou

Právní novinky

Deloitte Česká republika

Deloitte.

Právní novinky
březen 2016

Jaké změny nás čekají v právní úpravě pro oblast kybernetické bezpečnosti

Že to Evropa s kybernetickou a online bezpečností myslí vážně svědčí i prosincové dohody o znění směrnice o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informací v Unii (NIS), jakož i dohoda v rámci tzv. trialogu o znění obecného nařízení o ochraně dat (GDPR).

Ochrana před stále častěji se opakujícími kybernetickými útoky však dlouho byla jednou z priorit ČR v rámci potlačování bezpečnostních hrozeb. Ještě před přijetím příslušné evropské úpravy směrnice NIS Česká republika následovala země, jako jsou Estonsko a Maďarsko, a přijala samostatný zákon o kybernetické bezpečnosti (ZOKB).

ZOKB nabyl účinnosti 1. ledna 2015 a obsahuje ucelenou právní úpravu kybernetické bezpečnosti, která je svou komplexností v rámci EU docela unikátní. Tento právní předpis stanovuje minimální požadavky na prevenci před kybernetickými útoky pro informační a komunikační systémy ze soukromoprávní i veřejnoprávní sféry, které jsou zásadní pro fungování státu (např. informační systém katastru nemovitostí, registr vozidel, informační systémy větších elektráren, tepláren, vodních děl, plynovodu atd).

Zákon vymezuje opatření nutná ke zvýšení odolnosti těchto systémů před rostoucím počtem kybernetických útoků a zavádí povinnost bezpečnostní incidenty hlásit s cílem zajistit rychlou reakci. Nezavádí v rámci bezpečnostních opatření žádné nové postupy, ale vychází ze standardů ISO, které jsou u některých povinných subjektů již zavedeny. Místo citelných sankcí za nedodržení povinností zákon sází na důvěru mezi povinnými subjekty a dohledovými pracovišti, vládním a národním CERTem, a jejich efektivní spolupráci při řešení případných bezpečnostních incidentů.

Jaké změny nás čekají v souvislosti s přijetím směrnice NIS?
Při schvalování znění směrnice NIS se intenzivně diskutovalo nad okruhem subjektů, kterých by se směrnice měla dotýkat. Do seznamu povinných subjektů by kromě těch určených dle současných právních předpisů (Jedná se zejména o subjekty kritické informační infrastruktury definované na základě ZOKB a novelizovaného nařízení vlády č.432/2010 Sb. o kritériích pro určení prvku kritické infrastruktury.) měli přibýt i klíčoví poskytovatelé služeb informační společnosti. Jsou jimi „poskytovatelé digitálních služeb", jako například platformy pro elektronické obchodování, internetové platební brány, online vyhledávače, poskytovatelé cloud computingu.

Narušení těchto služeb totiž brání poskytování dalších služeb kritické infrastruktury. Povinnosti by se však neměly týkat malých podniků do 50 zaměstnanců a obratem do 10 milionů EUR. Směrnice NIS počítá s rozšířením i na poskytovatele digitální infrastruktury, jako jsou například výměnné uzly internetu, poskytovatelé DNS domén a klíčoví registrátoři domén. S těmito prvky však rámcově počítá i česká úprava ZOKB.
Mezi nové povinné subjekty dle směrnice NIS by ale neměli patřit původně zvažovaní mobilní operátoři, na něž se vztahují povinnosti dle jiných evropských předpisů. Členské státy však mohou přijmout přísnější opatření, což by odpovídalo současné právní úpravě ZOKB, resp. příslušných podzákonných předpisů, na základě kterých lze mezi povinné subjekty zařadit i mobilní operátory.

Vlastník nebo provozovatel kritické informační infrastruktury?
I dle současného znění ZOKB je mnohdy problém definovat, kdo je povinným subjektem kritické informační infrastruktury, tj. kdo odpovídá za dodržování povinností stanovených ZOKB. Je to vlastník, nebo

Deloitte.

provozovatel daného prvku kritické informační infrastruktury? Ne vždy se totiž musí jednat o jednu a tutéž osobu. Problém nastává tehdy, pokud, zjednodušeně řečeno, vlastníkem elektrárny (která je prvkem kritické infrastruktury) je jiná právní entita než vlastník, resp. provozovatel informačního systému (prvek kritické informační infrastruktury), který fungování předmětné elektrárny řídí. Není tedy zcela zřejmé, kdo je povinným subjektem podle zákona v situaci, když byla tato činnost (provozování informačního systému řídícího elektrárnu) např. outsourcována.

Český ZOKB, resp. důvodová zpráva k němu, počítá s tím, že povinným subjektem je/bude ten, kdo fakticky určuje účel příslušného systému a podmínky jeho provozování, „typicky" jeho vlastník. Nastalou situaci lze tedy řešit v rámci jednání mezi potenciálním subjektem a NBÚ, který je oprávněn subjekty kritické informační infrastruktury určovat. Nasměřovat na této křižovatce by mohla i směrnice NIS, která stanoví, že odpovědným subjektem je vlastník kritické infrastruktury (v našem příkladu vlastník elektrárny). Optimální by bylo v tomto duchu ZOKB upravit a definovat jasněji, kdo je povinným subjektem.

Co znamená ohlašování incidentů a událostí

V praxi se častokrát setkáváme s nejistotou povinných subjektů, jaká narušení kybernetické bezpečnosti mají ohlašovat národnímu nebo vládnímu CERTu. Je třeba rozlišovat mezi kybernetickou bezpečnostní UDÁLOSTÍ a kybernetickým bezpečnostním INCIDENTEM. Událost může způsobit narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb, bezpečnosti a integrity sítí elektronických komunikací. ZOKB sice zavádí povinnost detekovat bezpečnostní události, ale povinnost něco hlásit národnímu nebo vládnímu CERTu se týká až kybernetických bezpečnostních incidentů. Kybernetická bezpečnostní událost se však může změnit v bezpečnostní incident.
Kybernetický bezpečnostní incident totiž představuje faktické narušení bezpečnosti informací v informačních systémech nebo narušení bezpečnosti služeb anebo bezpečnosti a integrity sítí elektronických komunikací v důsledku kybernetické bezpečnostní události.
O detekovaných bezpečnostních událostech si subjekty mají vést evidenci jen pro svou vlastní potřebu. Pokud ale tuto detekční povinnost budou ignorovat, nehrozí jim žádná sankce. Povinné subjekty by si proto měly uvědomit, že co je u jednoho subjektu bezpečnostní událostí s nízkým stupněm ohrožení, která se do bezpečnostního incidentu nepřerodí a zůstane jen na úrovni „hrozby", může být u jiného subjektu významným bezpečnostním incidentem s velkým dopadem.

S povinností hlásit incidenty přichází i nařízení GDPR, avšak trochu v jiném kontextu. Zatímco cílem nařízení GDPR je ochrana osobních údajů, cílem směrnice NIS je ochrana sítí. S tím souvisí i povinnosti správců údajů přijmout opatření (podobného charakteru, jako stanoví ZOKB) k ochraně osobních údajů, přičemž směrnice NIS požaduje od operátorů ochranu sítí s cílem zajistit poskytování služeb. Ačkoli se tyto účely někdy prolínají, jsou i oblasti, kdy budou ochranná opatření sledovat opačný cíl.

Obdobně to platí i ohledně povinností ohlašovat incidenty. Dle GDPR budou správci údajů povinni notifikovat příslušný orgán do 72 hodin od zjištění incidentu, to však neplatí v situaci, kdy narušení bezpečnosti údajů nezpůsobí riziko pro práva a svobody jednotlivců. Z toho vyplývá, že notifikační povinnost je na místě pouze v případě ohrožení práv jednotlivců.

Deloitte.

Povinnost notifikovat incident podle směrnice NIS však nastává v situaci, když dojde k závažnému přerušení poskytování služeb, tj. bez ohledu na to, jaký dopad to má na případný únik/ztrátu dat/informací. Může však nastat situace, že incident bude nutné notifikovat jak na základě nařízení GDPR tak i směrnice NIS, nebo naopak jen na základě jednoho z nich.
ZOKB bude s největší pravděpodobností v nejbližší době muset čelit změnám v důsledku nově přijaté evropské úpravy, jakož i s ohledem na praktické zkušenosti s ním. Kromě změn vyplývajících ze směrnice NIS by se zákonodárce mohl zamyslet i nad stanovením dalších odvětvových kritérií, např. s ohledem na úpravu v jiných členských státech EU (např. chemický a farmaceutický průmysl a jiné). Změny mohou doznat i sankce za porušení ZOKB. Směrnice NIS totiž stanoví povinnost pro členské státy, aby sankce byly účinné, přiměřené a odrazující. Nutno podotknout že nejvyšší současná sankce podle ZOKB je pouhých otknout že nejvyšší současná sankce podle ZOKB je 100 000,innost pro členské státy, aby sankce byly dostatečně na které100 000 korun českých a je tedy otázkou, zda taková sankce je opravdu účinná, přiměřená a odrazující.

Jaroslava Kračúnová
+420 246 042 851
jkracunova@deloittece.com

Deloitte.

Dodatečné daňové přiznání vs. daňová kontrola: Jak mají společnosti postupovat, pokud se u nich plánuje daňová kontrola?

V současné době zaznamenáváme trend, kdy orgány finanční správy v čele s Generálním finančním ředitelstvím přehodnocují svůj dosavadní přístup ke zdaňování některých oblastí a u dotčených společností pak zahajují daňové kontroly. V těchto případech jsou společnosti postaveny do situace, kdy se musí v relativně krátké době rozhodnout, zda vyčkají výsledku daňové kontroly nebo podají dodatečné daňové přiznání tak, aby se vyhnuly uložení penále. Tento příspěvek přináší několik poznámek k tomu, co by měla společnost v takovýchto situacích zvážit.

V první řadě je nutné poznamenat, že pokud má správce daně jakékoliv indicie o tom, že je nutné změnit poslední zjištěnou daň, měl by podle judikatury Nejvyššího správního soudu ještě před zahájením daňové kontroly vyzvat společnost k podání dodatečného daňového přiznání a umožnit jí tak, aby se vyhnula uložení vysokého penále (viz NSS, rozsudek ze dne 6. května 2015, č. j. 2 Afs 209/2014–23). V případě, kdy společnost sama dodatečně přizná zvýšenou daňovou povinnost, jí totiž na rozdíl od daňové kontroly nemůže být uloženo penále.

Na výzvu k podání dodatečného daňového přiznání by měla společnost reagovat, v opačném případě totiž může správce daně doměřit daň podle pomůcek. Společnost však nemusí s výkladem správce daně vždy souhlasit. Nejvyšší správní soud k tomuto uvedl, že pokud daňový subjekt nesouhlasí s obsahem, resp. s důvody výzvy k předložení dodatečného daňového přiznání, a tento nesouhlas správci daně ve lhůtě stanovené ve výzvě písemně sdělí, není správce daně bez dalšího oprávněn doměřit daň dle pomůcek (viz NSS, rozsudek ze dne 6. srpna 2015, č. j. 9 Afs 66/2015–36). Jinými slovy, společnost musí mít možnost vyhodnotit svou situaci a rozhodnout se, zda podá dodatečné daňové přiznání a vyhne se tak riziku penále, anebo zda je připravena obhájit svou původně tvrzenou daňovou povinnost před soudem.

V nedávné době Nejvyšší správní soud v této souvislosti také potvrdil, že je zcela legitimní, pokud společnost provede před plánovanou daňovou kontrolu interní audit a den před zahájením daňové kontroly podá dodatečné daňové přiznání (viz NSS, rozsudek ze dne 9. prosince 2015, č. j. 10 Afs 105/2015–44). Za okamžik zahájení daňové kontroly přitom nelze považovat sepsání protokolu o jejím zahájení, v němž je daňový subjekt pouze seznámen se skutečností, že u něj bude v následujícím období daňová kontrola prováděna, ale správce daně musí skutečně začít zjišťovat skutkový stav. Do té doby, než se tak stane, má proto společnost možnost sama dodatečně přiznat své daňové povinnosti (NSS, rozsudek ze dne 20. 6. 2005, č. j. 5 Afs 36/2003–87).

Pokud u Vás správce daně plánuje provést daňovou kontrolu či máte informace o tom, že přehodnotil svůj dosavadní přístup k některým otázkám, jsme připraveni vyhodnotit situaci a pomoci Vám zvolit ten nejvhodnější postup.

Tomáš Babáček
+420 246 042 814
tbabacek@deloittece.com

Jiřina Neumannová
+420 246 042 430
jneumannova@deloittece.com

Deloitte.

Právní novinky
březen 2016

Návrh zákona o centrální evidenci účtů schválen vládou

Vláda České republiky schválila dne 3. února 2016 návrh zákona o centrální evidenci účtů a souvisejícího změnového zákona, které bude nyní projednávat Poslanecká sněmovna. Podle návrhu má vzniknout centrální evidence bankovních účtů vedených úvěrovými institucemi v ČR ve správě České národní banky.

Registr bude obsahovat základní údaje o bankovních účtech a jejich vlastnících, nikoliv však dostupný zůstatek či informace o finančních operacích. Systém nebude napojen na jiné evidence, například na základní registry. Povinnost poskytovat údaje do registru budou mít banky, pobočky zahraničních bank, spořitelní a úvěrová družstva, a to pod hrozbou pokuty až do maximální výše 10 mil. Kč. Dle návrhu zákona budou povinné osoby muset údaje ČNB zasílat elektronicky do 12:00 každého pracovního dne. V návrhu zákona je stanoven seznam výlučně oprávněných orgánů, které mohou informace z evidence žádat. Jedná se o orgány činné v trestním řízení, tajné služby a orgány spadající pod Ministerstvo financí, které je hlavním autorem návrhu. Tyto orgány budou povinny vést evidenci žádostí a uchovávat údaje v ní po dobu pěti let. ČNB pak údaje bude uchovávat po dobu 10 let od zrušení účtu.

Ačkoliv má návrh zákona řadu kritiků, kteří jej považují za další zásah do soukromí občanů, Ministerstvo financí obhajuje nutnost zákona efektivnějším bojem proti daňovým únikům a upozorňuje, že vznik této evidence je doporučován i unijními předpisy. Oprávněným subjektům navíc odpadne nutnost kontaktovat desítky úvěrových institucí a informace budou předány výrazně rychleji, než tomu bylo doposud (ČNB má povinnost na žádost odpovědět do 24 hodin).

Úvěrové instituce si tedy budou muset pořídit software pro přenos požadovaných dat, na druhou stranu ale ušetří za zpracování žádostí o poskytnutí údajů. Evidence by však dle předpokladů ministerstva měla být spuštěna teprve v polovině roku 2018, aby úvěrové instituce měly dostatek času na přípravu svých systémů.

Jan Procházka
+420 246 042 913
jprochazka@deloittece.com

Deloitte.

Právní novinky
březen 2016

- Jaké změny nás čekají v právní úpravě pro oblast kybernetické bezpečnosti
- Dodatečné daňové přiznání vs. daňová kontrola: Jak mají společnosti postupovat, pokud se u nich plánuje daňová kontrola?
- Návrh zákona o centrální evidenci účtů schválen vládou

Kontakty

Máte-li zájem o další informace ohledně služeb poskytovaných společností Deloitte v České republice, obraťte se prosím na odborníky z právního oddělení:

Ambruz & Dark Deloitte Legal s.r.o., advokátní kancelář
Nile House
Karolinská 654/2
186 00 Praha 8 - Karlín
Česká republika
Tel.: +420 246 042 100
Fax: +420 246 042 030

www.deloittelegal.cz

Přihlaste se k odběru dReportu a jiných newsletterů a pozvánek zde
http://www2.deloitte.com/cz/subscribe

Deloitte.