V l á d n í n á v r h

ZÁKON

ze dne 2024,

kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti

Parlament se usnesl na tomto zákoně České republiky:

ČÁST PRVNÍ
Změna zákona o bankách

Čl. I

Zákon č. 21/1992 Sb., o bankách, ve znění zákona č. 264/1992 Sb., zákona č. 292/1993 Sb., zákona č. 156/1994 Sb., zákona č. 83/1995 Sb., zákona č. 84/1995 Sb., zákona č. 61/1996 Sb., zákona č. 306/1997 Sb., zákona č. 16/1998 Sb., zákona č. 127/1998 Sb., zákona č. 165/1998 Sb., zákona č. 120/2001 Sb., zákona č. 239/2001 Sb., zákona č. 319/2001 Sb., zákona č. 126/2002 Sb., zákona č. 453/2003 Sb., zákona č. 257/2004 Sb., zákona č. 439/2004 Sb., zákona č. 377/2005 Sb., zákona č. 413/2005 Sb., zákona č. 56/2006 Sb., zákona č. 57/2006 Sb., zákona č. 62/2006 Sb., zákona č. 70/2006 Sb., zákona č. 159/2006 Sb., zákona č. 189/2006 Sb., zákona č. 443/2006 Sb., nálezu Ústavního soudu, vyhlášeného pod č. 37/2007 Sb., zákona č. 120/2007 Sb., zákona č. 296/2007 Sb., zákona č. 126/2008 Sb., zákona č. 216/2008 Sb., zákona č. 230/2008 Sb., zákona č. 254/2008 Sb., zákona č. 433/2008 Sb., zákona č. 215/2009 Sb., zákona č. 227/2009 Sb., zákona č. 230/2009 Sb., zákona č. 281/2009 Sb., zákona č. 285/2009 Sb., zákona č. 287/2009 Sb., zákona č. 156/2010 Sb., zákona č. 160/2010 Sb., zákona č. 409/2010 Sb., zákona č. 41/2011 Sb., zákona č. 73/2011 Sb., zákona č. 139/2011 Sb., zákona č. 188/2011 Sb., zákona č. 263/2011 Sb., zákona č. 420/2011 Sb., zákona č. 428/2011 Sb., zákona č. 470/2011 Sb., zákona č. 37/2012 Sb., zákona č. 254/2012 Sb., zákona č. 396/2012 Sb., zákona č. 227/2013 Sb., zákona č. 241/2013 Sb., zákona č. 303/2013 Sb., zákona č. 135/2014 Sb., zákona č. 219/2015 Sb., zákona č. 220/2015 Sb., zákona č. 375/2015 Sb., zákona č. 258/2016 Sb., zákona č. 301/2016 Sb., zákona č. 302/2016 Sb., zákona č. 368/2016 Sb., zákona č. 183/2017 Sb., zákona č. 204/2017 Sb., zákona č. 371/2017 Sb., zákona č. 39/2020 Sb., zákona č. 49/2020 Sb., zákona č. 119/2020 Sb., zákona č. 238/2020 Sb., zákona č. 338/2020 Sb., zákona č. 174/2021 Sb., zákona č. 261/2021 Sb., zákona č. 353/2021 Sb., zákona č. 96/2022 Sb., zákona č. 471/2022 Sb., zákona č. 35/2023 Sb., zákona č. 407/2023, zákona č. 417/2023 Sb., zákona č. 85/2024 Sb. a zákona č. 107/2024 Sb., se mění takto:

1. V § 38 odst. 3 se na konci písmene o) slovo „nebo“ zrušuje.

2. V § 38 odst. 3 se na konci písmene p) tečka nahrazuje slovem „, nebo“ a vkládá se písmeno q), které zní:

„q) Národního úřadu pro kybernetickou a informační bezpečnost při prověřování rizik spojených s dodavatelem poskytovatele strategicky významné služby podle zákona o kybernetické bezpečnosti.“.

CELEX 32009L0044, 32013L0036, 32013R0575

ČÁST DRUHÁ
Změna zákona o poštovních službách

Čl. II

Zákon č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění zákona č. 517/2002 Sb., zákona č. 225/2003 Sb., zákona č. 501/2004 Sb., zákona č. 95/2005 Sb., zákona č. 413/2005 Sb., zákona č. 444/2005 Sb., zákona č. 264/2006 Sb., zákona č. 110/2007 Sb., zákona č. 41/2009 Sb., zákona č. 281/2009 Sb., zákona č. 285/2009 Sb., zákona č. 153/2010 Sb., zákona č. 329/2011 Sb., zákona č. 89/2012 Sb., zákona č. 221/2012 Sb., zákona č. 212/2013 Sb., zákona č. 258/2014 Sb., zákona č. 319/2015 Sb., zákona č. 378/2015 Sb., zákona č. 250/2016 Sb., zákona č. 183/2017 Sb., zákona č. 202/2019 Sb., zákona č. 164/2020 Sb. a zákona č. 374/2021 Sb., se mění takto:

1. V § 33 se za odstavec 2 vkládá nový odstavce 3, který zní:

„(3) Držitel poštovní licence je povinen bez zbytečného odkladu informovat Úřad o ohrožení nebo narušení bezpečnosti poštovní sítě, poskytování základních služeb nebo přístupu k prvkům poštovní infrastruktury a k zvláštním službám souvisejícím s provozováním poštovní infrastruktury podle § 34. Tato povinnost se neuplatní, pokud má narušení bezpečnosti a integrity těchto sítí a služeb původ v kybernetickém prostoru, a to v rozsahu, ve kterém se na držitele poštovní licence vztahují obdobné informační povinnosti podle zákona o kybernetické bezpečnosti.“.

Dosavadní odstavce 3 až 9 se označují jako odstavce 4 až 10.

CELEX 32022L2555, 32008L0006

2. V § 33 odst. 6 se slova „odstavce 6“ nahrazují slovy „odstavce 7“.

3. V § 33 odst. 7 se slova „odstavce 5“ nahrazují slovy „odstavce 6“.

CELEX 32008L0006

4. V § 33 odst. 10 se slova „odstavce 8“ nahrazují slovy „odstavce 9“.

5. Za § 36a se vkládá nový § 36b, který včetně nadpisu zní:

„§ 36b

Spolupráce s Národním úřadem pro kybernetickou a informační bezpečnost

Úřad a Národní úřad pro kybernetickou a informační bezpečnost si vzájemně poskytují podněty, informace a jiné formy součinnosti potřebné k plnění úkolů, které jim stanoví právní předpisy. Při předávání informací je příjemce povinen zajistit stejnou úroveň důvěrnosti jako předávající.“.

6. V § 37a odst. 3 se za písmeno b) vkládá nové písmeno c), které zní:

„c) nesplní informační povinnost podle § 33 odst. 3,“.

Dosavadní písmena c) až g) se označují jako písmena d) až h).

7. V § 37a odst. 3 písm. d) se text „odst. 4“ nahrazuje textem „odst. 5“.

8. V § 37a odst. 3 písm. e) se slova „odst. 5, 7, 8 nebo 9“ nahrazují slovy „odst. 6, 8, 9 nebo 10“.

9. V § 37a odst. 6 písm. a) se text „písm. e)“ nahrazuje textem „písm. f)“.

10. V § 37a odst. 6 písm. b) se slova „písm. f) nebo g)“ nahrazují slovy „písm. e), g) nebo h)“.

11. V § 41 odst. 1 se text „odst. 4“ nahrazuje textem „odst. 5“.

ČÁST TŘETÍ
Změna zákona o informačních systémech veřejné správy

Čl. III

Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění zákona č. 517/2002 Sb., zákona č. 413/2005 Sb., zákona č. 444/2005 Sb., zákona č. 70/2006 Sb., zákona č. 81/2006 Sb., zákona č. 110/2007 Sb., zákona č. 269/2007 Sb., zákona č. 130/2008 Sb., zákona č. 190/2009 Sb., zákona č. 223/2009 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 263/2011 Sb., zákona č. 18/2012 Sb., zákona č. 167/2012 Sb., zákona č. 64/2014 Sb., zákona č. 298/2016 Sb., zákona č. 301/2016 Sb., zákona č. 368/2016 Sb., zákona č. 104/2017 Sb., zákona č. 183/2017 Sb., zákona č. 195/2017 Sb., zákona č. 205/2017 Sb., zákona č. 251/2017 Sb., zákona č. 99/2019 Sb., zákona č. 12/2020 Sb., zákona č. 261/2021 Sb., zákona č. 471/2022 Sb. a zákona č. 1/2024 Sb., se mění takto:

1. V § 2 odst. 2 písmeno a) zní:

„a) bezpečnostní úrovní bezpečnostní úroveň informačního systému veřejné správy vyjadřující možné dopady kybernetického bezpečnostního incidentu na informační systém veřejné správy, k zajištění jehož provozu má být využíván cloud computing,“.

2. V § 2 se na konci odstavce 2 tečka nahrazuje čárkou a doplňuje se písmeno g), které zní:

„g) bezpečnostními pravidly pravidla pro orgány veřejné správy využívající služby poskytovatelů cloud computingu stanovující minimální požadavky pro využívání služby cloud computingu orgánem veřejné správy s cílem zajistit bezpečnost informací.“.

3. V § 4 odst. 2 se na konci textu písmene a) doplňují slova „ , s výjimkou povinností stanovených v § 6n písm. b) až f) a § 6l odst. 3“.

4. V § 5a odst. 2 se věta poslední nahrazuje větou „Strukturu a náležitosti informační koncepce orgánu veřejné správy, jakož i postupy orgánů veřejné správy při jejím vytváření, vydávání a při vyhodnocování jejího dodržování, požadavky na řízení informačních systémů veřejné správy, včetně dekomponování informačních systémů veřejné správy, technické požadavky na informační systémy veřejné správy a pravidla pro strukturování dat v informačních systémech veřejné správy stanoví prováděcí právní předpis.“.

5. § 5b zní:

„§ 5b

Správci informačních systémů veřejné správy, kteří nejsou poskytovateli regulované služby podle zákona o kybernetické bezpečnosti, jsou povinni na jimi spravované informační systémy veřejné správy zavádět bezpečnostní opatření pro poskytovatele regulované služby v režimu nižších povinností podle § 6, 14 a 15 zákona o kybernetické bezpečnosti, a to přiměřeně s ohledem na možné dopady narušení důvěrnosti, integrity a dostupnosti konkrétního informačního systému veřejné správy na činnost jeho správce a jeho schopnost poskytovat své služby občanům, a dále vhodnost a proveditelnost těchto opatření.“.

6. V § 6i odst. 2 písm. e) se za text „§ 6n“ vkládá text „písm. a)“.

7. V § 6i odstavec 3 zní:

„(3) Národní úřad pro kybernetickou a informační bezpečnost

a) kontroluje, zda cloud computing poskytovaný orgánům veřejné správy splňuje požadavky podle § 6n písm. b) až f),

b) kontroluje zařazení informačního systému veřejné správy do bezpečnostní úrovně podle § 6l odst. 3,

c) kontroluje zajištění dodržování bezpečnostních pravidel orgánem veřejné správy při využívání služby cloud computingu podle § 6l odst. 3.“.

8. V § 6l se na konci odstavce 3 doplňují věty „Orgán veřejné správy je povinen před uzavřením smlouvy s poskytovatelem cloud computingu zařadit informační systém veřejné správy nebo jeho část, k zajištění jehož provozu má být cloud computing využíván, do bezpečnostní úrovně s ohledem na povahu dotčeného informačního systému veřejné správy podle prováděcího právního předpisu. Orgán veřejné správy je dále povinen zajišťovat, že budou po celou dobu využívání služeb cloud computingu dodržována bezpečnostní pravidla.“.

9. V § 6n písm. c) se slova „postupovat podle bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu podle právního předpisu upravujícího kybernetickou bezpečnost“ nahrazují slovy „zajistit dodržování bezpečnostních pravidel stanovených prováděcím právním předpisem“.

10. V § 6q odst. 5 písm. c), § 6t odst. 6 písm. b) a d) až g) a § 6t odst. 7 písm. c) a e) až h) se slova „upravujícím kybernetickou bezpečnost“ nahrazují slovy „vydaným podle § 12 odst. 2“.

11. Na konci nadpisu § 7 se doplňují slova „**a orgánů veřejné správy**“.

12. V § 7 se za odstavec 3 vkládají nové odstavce 4 a 5, které znějí:

„(4) Poskytovatel cloud computingu se dopustí přestupku tím, že poskytuje orgánu veřejné správy nebo poskytovateli státního cloud computingu cloud computing, který nesplňuje požadavky na cloud computing využívaný orgánem veřejné správy podle § 6n.

(5) Orgán veřejné správy se dopustí přestupku tím, že
a) využívá cloud computing v rozporu s § 6l odst. 1,
b) nesplní ve stanovené lhůtě povinnost ukončit využívání cloud computingu podle § 6l odst. 2,
c) nesplní povinnost zařadit informační systém nebo jeho část do bezpečnostní úrovně podle § 6l odst. 3, nebo
d) nezajišťuje dodržování bezpečnostních pravidel podle § 6l odst. 3.“.

Dosavadní odstavec 4 se označuje jako odstavec 6.

13. V § 7 odst. 6 se vkládá nové písmeno a), které zní:

„a) 10 000 000 Kč, jde-li o přestupek podle odstavce 4 nebo 5,“.

Dosavadní písmena a) až c) se označují jako písmena b) až d).

14. V § 9e odst. 3 se slova „správci a provozovateli významného informačního systému“ zrušují.

15. V § 12 odst. 1 písm. b) se slova „bezpečnostních úrovní a“ zrušují.

16. V § 12 se na konci odstavce 2 tečka nahrazuje čárkou a doplňují se písmena g) a h), která znějí:

„g) bezpečnostní úrovně informačních systémů veřejné správy,
h) obsah a rozsah bezpečnostních pravidel pro orgány veřejné správy využívající služeb cloud computingu podle § 6l odst. 3.“.

ČÁST ČTVRTÁ
Změna zákona o elektronických komunikacích

Čl. IV

Zákon č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění zákona č. 290/2005 Sb., zákona č. 361/2005 Sb., zákona č. 186/2006 Sb., zákona č. 235/2006 Sb., zákona č. 310/2006 Sb., zákona č. 110/2007 Sb., zákona č. 261/2007 Sb., zákona č. 304/2007 Sb., zákona č. 124/2008 Sb., zákona č. 177/2008 Sb., zákona č. 189/2008 Sb., zákona č. 247/2008 Sb., zákona č. 384/2008 Sb., zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 153/2010 Sb.,

nálezu Ústavního soudu, vyhlášeného pod č. 94/2011 Sb., zákona č. 137/2011 Sb., zákona č. 341/2011 Sb., zákona č. 375/2011 Sb., zákona č. 420/2011 Sb., zákona č. 457/2011 Sb., zákona č. 468/2011 Sb., zákona č. 18/2012 Sb., zákona č. 19/2012 Sb., zákona č. 142/2012 Sb., zákona č. 167/2012 Sb., zákona č. 273/2012 Sb., zákona č. 214/2013 Sb., zákona č. 303/2013 Sb., zákona č. 181/2014 Sb., zákona č. 234/2014 Sb., zákona č. 250/2014 Sb., zákona č. 258/2014 Sb., zákona č. 318/2015 Sb., zákona č. 378/2015 Sb., zákona č. 222/2016 Sb., zákona č. 298/2016 Sb., zákona č. 183/2017 Sb., zákona č. 194/2017 Sb., zákona č. 225/2017 Sb., zákona č. 252/2017 Sb., zákona č. 287/2018 Sb., zákona č. 277/2019 Sb., zákona č. 311/2019 Sb., zákona č. 403/2020 Sb., zákona č. 150/2021 Sb., zákona č. 261/2021 Sb., zákona č. 270/2021 Sb., zákona č. 284/2021 Sb., zákona č. 374/2021 Sb., zákona č. 152/2023 Sb., zákona č. 202/2023 Sb. a zákona č. 349/2023 Sb., se mění takto:

1.V § 6 se doplňuje odstavec 6, který zní:

„(6) Úřad rozhodne na základě žádosti o změně nebo zrušení regulačního opatření uloženého rozhodnutím vydaným na základě tohoto zákona v případě, že plnění podmínek nebo povinností stanovených v takovém rozhodnutí znemožňuje zcela nebo zčásti plnit povinnosti uvedené v protiopatření nebo opatření obecné povahy vydaných podle zákona o kybernetické bezpečnosti.“.

2. V § 22a odst. 3 se slova „odstavce 5“ nahrazují slovy „odstavce 6“.

3. V § 22a se za odstavec 4 vkládá nový odstavec 5, který zní:

„(5) Předseda Rady může rozhodnout po konzultaci podle § 130 o změně přídělu rádiových kmitočtů, jestliže je to nezbytné pro plnění protiopatření nebo plnění účelu opatření obecné povahy vydaného podle zákona o kybernetické bezpečnosti. Postup podle § 6 odst. 6 tím není dotčen.“.

Dosavadní odstavec 5 se označuje jako odstavec 6.

CELEX 32018L1972

4. V § 98 se doplňuje odstavec 9, který zní:

„(9) Povinnosti stanovené nebo uložené na základě odstavců 1, 3, 4 a 6 až 8 se neuplatní v případě podnikatele zajišťujícího veřejnou komunikační síť nebo poskytujícího veřejně dostupnou službu elektronických komunikací, pokud má narušení bezpečnosti a integrity těchto sítí a služeb původ v kybernetickém prostoru, a to v rozsahu, ve kterém se na něj vztahují obdobné informační povinnosti podle zákona o kybernetické bezpečnosti.“.

CELEX 32022L2555

ČÁST PÁTÁ
Změna zákona o provádění mezinárodních sankcí

Čl. V

Zákon č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 139/2011 Sb., zákona č. 167/2012 Sb., zákona č. 399/2012 Sb., zákona č. 377/2015 Sb., zákona č. 298/2016 Sb., zákona č. 368/2016 Sb., zákona č. 183/2017 Sb., zákona č. 261/2021 Sb. a zákona č. 240/2022 Sb., se mění takto:

1. V § 16 odst. 4 písm. m) se slovo „nebo“ nahrazuje čárkou.

2. V § 16 se na konci odstavce 4 tečka nahrazuje slovem „, nebo“ a doplňuje se písmeno o), které zní:

„o) Národnímu úřadu pro kybernetickou a informační bezpečnost při prověřování rizik spojených s dodavatelem podle zákona o kybernetické bezpečnosti.“.

3. V § 16 se doplňuje odstavec 7, který zní:

„(7) Výjimky uvedené v odstavci 4 písm. b) až o) se uplatní jen v nezbytně nutném rozsahu podle účelu poskytované informace. Nelze je uplatnit, pokud by poskytnutí informací mohlo zmařit nebo ohrozit šetření podle tohoto zákona nebo probíhající trestní řízení, nebo jestliže by poskytnutí informací bylo zjevně nepřiměřené oprávněným zájmům osoby, jíž se informace týká, nebo účelu, pro který byla žádost podána.“.

ČÁST ŠESTÁ
Změna zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

Čl. VI

Zákon č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění zákona č. 227/2009 Sb., zákona č. 281/2009 Sb., zákona č. 285/2009 Sb., zákona č. 199/2010 Sb., zákona č. 139/2011 Sb., zákona č. 420/2011 Sb., zákona č. 428/2011 Sb., zákona č. 457/2011 Sb., zákona č. 18/2012 Sb., zákona č. 377/2012 Sb., zákona č. 399/2012 Sb., zákona č. 241/2013 Sb., zákona č. 303/2013 Sb., zákona č. 257/2014 Sb., zákona č. 166/2015 Sb., zákona č. 377/2015 Sb., zákona č. 188/2016 Sb., zákona č. 243/2016 Sb., zákona č. 368/2016 Sb., zákona č. 183/2017 Sb., zákona č. 371/2017 Sb., zákona č. 35/2018 Sb., zákona č. 94/2018 Sb., zákona č. 111/2019 Sb., zákona č. 49/2020 Sb., zákona č. 527/2020 Sb., zákona č. 34/2021 Sb., zákona č. 172/2023 Sb., zákona č. 1/2024 Sb. a zákona č. 107/2024 Sb., se mění takto:

1. V § 39 se na konci odstavce 1 tečka nahrazuje čárkou a doplňuje se písmeno r), které zní:

„r) Národnímu úřadu pro kybernetickou a informační bezpečnost při prověřování rizik spojených s dodavatelem podle zákona o kybernetické bezpečnosti.“.

2. V § 39 odst. 4 úvodní části ustanovení se text „q)“ nahrazuje textem „r)“.

CELEX 32015L0849, 32019L1153

ČÁST SEDMÁ
Změna daňového řádu

Čl. VII

V § 53 zákona č. 280/2009 Sb., daňový řád, ve znění zákona zákonného opatření Senátu č. 344/2013 Sb., zákona č. 368/2016 Sb., zákona č. 170/2017 Sb., zákona č. 94/2018 Sb., zákona č. 283/2020 Sb. a zákona č. 527/2020 Sb., se na konci odstavce 1 tečka nahrazuje čárkou a doplňuje se písmeno n), které zní:

„n) Národnímu úřadu pro kybernetickou a informační bezpečnost při prověřování rizik spojených s dodavatelem podle zákona o kybernetické bezpečnosti.“.

ČÁST OSMÁ
Změna zákona o Celní správě České republiky

Čl. VIII

V § 27 odst. 3 zákona č. 17/2012 Sb., o Celní správě České republiky, ve znění zákona č. 283/2020 Sb., se za slovo „republiky,“ vkládají slova „Národnímu úřadu pro kybernetickou a informační bezpečnost,“.

ČÁST DEVÁTÁ
Změna zákona o prověřování zahraničních investic

Čl. IX

Zákon č. 34/2021 Sb., o prověřování zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic), ve znění zákona č. …/2024 Sb., se mění takto:

1. V § 7 písm. c) se slova „správcem informačního systému kritické informační infrastruktury, správcem komunikačního systému kritické informační infrastruktury, správcem informačního systému základní služby nebo provozovatelem základní služby[5)]“ nahrazují slovy „poskytovatelem regulované služby v režimu vyšších povinností[5)]“.

Poznámka pod čarou č. 5 zní:
„[5)] Zákon č. .../2024 Sb., o kybernetické bezpečnosti.“.

2. § 20a včetně nadpisu zní:

„§ 20a

Výjimky z povinnosti mlčenlivosti

(1) Povinnost zaměstnanců ministerstva pověřených vedením řízení nebo konzultací podle tohoto zákona zachovávat mlčenlivost podle § 20 se neuplatní v rámci spolupráce ministerstva s

a) Úřadem podle právního předpisu upravujícího některé vztahy v oblasti veřejné podpory[9)] a

b) Národním úřadem pro kybernetickou a informační bezpečnost při prověřování bezpečnosti dodavatelského řetězce podle právního předpisu upravujícího kybernetickou bezpečnost.

(2) Zaměstnanci Národního úřadu pro kybernetickou a informační bezpečnost jsou oprávněni informace získané v rámci spolupráce podle odstavce 1 písm. b) použít pouze při prověřování bezpečnosti dodavatelského řetězce a jsou povinni o nich zachovávat mlčenlivost.“.

CELEX 32019R0452

ČÁST DESÁTÁ
ÚČINNOST

Čl. X

Tento zákon nabývá účinnosti dnem 18. října 2024.

DŮVODOVÁ ZPRÁVA

A. Obecná část

Návrh zákona, kterým se mění některé zákony v souvislosti s přijetím zákona o kybernetické bezpečnosti (dále jen „návrh zákona“), je předkládán současně s návrhem nového zákona o kybernetické bezpečnosti (dále také jen „návrh ZKB“), který má za cíl nahradit dosavadní zákon č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „zákon č. 181/2014 Sb.“) a jeho prováděcí právní předpisy. Návrh ZKB je zároveň transpozičním předpisem směrnice Evropského parlamentu a Rady (EU) 2022/2555 ze dne 14. prosince 2022 o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii a o změně nařízení (EU) č. 910/2014 a směrnice (EU) 2018/1972 a o zrušení směrnice (EU) 2016/1148 (směrnice NIS 2). Právě v souvislosti s obsahem směrnice NIS 2 a dalšími změnami, které nastanou s účinností návrhu ZKB, je nutné změnit ustanovení některých účinných právních předpisů v České republice (dále jen „ČR“).

1. Zhodnocení platného právního stavu, včetně zhodnocení současného stavu ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Povinnosti upravené v návrhu ZKB se vztahují mimo jiné i na podnikatele zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací, kteří mají povinnost hlásit kybernetické bezpečnostní incidenty Národnímu úřadu pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) a spolupracovat s NÚKIB při jejich řešení a předcházení jim. Tito podnikatelé jsou ve vztahu k zajišťování bezpečnosti a integrity uvedené sítě a k zajišťování bezpečnosti uvedené služby vázáni také zákonem č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích), ve znění pozdějších předpisů (dále také jen „ZEK“), v rámci něhož mají povinnost hlásit (obecné) bezpečnostní incidenty Českému telekomunikačnímu úřadu (dále jen „ČTÚ“) a spolupracovat s ČTÚ při jejich řešení a předcházení jim. Vyvstává proto potřeba upravit vzájemný vztah návrhu ZKB a ZEK, a to změnou posledně zmíněného právního předpisu. Obdobně je tomu také v případě provozovatelů poštovních služeb podle zákona č. 29/2000 Sb., o poštovních službách a o změně některých zákonů (zákon o poštovních službách), ve znění pozdějších předpisů.

Dále platí, že návrh ZKB na rozdíl od zákona č. 181/2014 Sb. stanovuje jedinou povinnou osobu (poskytovatele regulované služby), a nestanovuje orgánům veřejné moci povinnost zajistit dodržování bezpečnostních pravidel v souvislosti s využíváním služby cloud computingu, stejně tak ani povinnost zařadit poptávaný cloud computing do bezpečnostní úrovně před uzavřením smlouvy s poskytovatelem cloud computingu. Návrh ZKB dále ruší vyhlášku č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci, ve znění pozdějšího předpisu. Z těchto skutečností vyplývá nutnost upravit znění zákona č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, ve znění pozdějších předpisů (dále jen „ZoISVS“). Společně s touto změnou se nabízí možnost využít v návrhu ZKB zakotvenou úroveň bezpečnostních opatření stanovených pro poskytovatele regulované služby v režimu nižších povinností tak, aby došlo ke sjednocenému stanovení standardu kybernetické bezpečnosti pro téměř celou veřejnou správu v ČR. Tento návrh má ambici dosáhnout nápravy doposud neutěšeného stavu, který byl popsán již v původní důvodové zprávě k zákonu č. 181/2014 Sb., v níž je uvedeno, že *„[v] oblasti veřejné správy neexistuje jednotný způsob stanovení bezpečnostních standardů, které by minimalizovaly potencionální škody vzniklé z kybernetických útoků“*.

Výše uvedenou změnu, obsaženou v návrhu ZKB, spočívající ve stanovení jediné povinné osoby, je nutné promítnout rovněž do znění zákona č. 34/2021 Sb., o prověřování

zahraničních investic a o změně souvisejících zákonů (zákon o prověřování zahraničních investic) (dále jen „ZoPZI“), neboť také tento právní předpis obsahově vychází z vymezení více povinných osob zákonem č. 181/2014 Sb.

V neposlední řadě platí, že zákon č. 21/1992 Sb., o bankách, ve znění pozdějších předpisů, (dále jen „ZoB“), ve vztahu k bankám, zákony č. 69/2006 Sb., o provádění mezinárodních sankcí, ve znění pozdějších předpisů (dále jen „ZPMS“), a č. 253/2008 Sb., o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu, ve znění pozdějších předpisů (dále jen „AML“, odvozeno z „*anti money laundering*“), ve vztahu k Finančnímu analytickému úřadu, zákon č. 280/2009 Sb., daňový řád, ve znění pozdějších předpisů (dále jen „daňový řád), ve vztahu ke správci daně, zákon č. 17/2012 Sb., o Celní správě České republiky, ve znění pozdějších předpisů (dále jen „ZCS“), ve vztahu k Celní správě ČR a ZoPZI ve vztahu k Ministerstvu průmyslu a obchodu vždy výslovně upravují situace, v nichž se poskytnutí informací uvedenými orgány nepovažuje za prolomení povinnosti mlčenlivosti, případně bankovního tajemství. S ohledem na skutečnost, že návrh ZKB zavádí mj. mechanismus prověřování rizik spojených s dodavatelem, a za účelem zajištění jeho řádného fungování v § 28 stanoví, že některé subjekty jsou povinny poskytovat NÚKIB informace, které získaly při své činnosti, případně poskytovat nezbytnou součinnost při zjišťování nezbytných informací potřebných pro činnost NÚKIB v rámci mechanismu prověřování rizik spojených s dodavatelem. Z tohoto důvodu je nutné u výše zmíněných subjektů novelizovat uvedené předpisy tak, aby poskytnutí těchto informací, případně poskytnutí součinnosti neznamenalo porušení povinnosti mlčenlivosti, resp. bankovního tajemství.

Současná právní úprava není diskriminační a nemá žádný dopad na rovnost mužů a žen.

2. Odůvodnění hlavních principů navrhované právní úpravy, včetně dopadů navrhovaného řešení ve vztahu k zákazu diskriminace a ve vztahu k rovnosti mužů a žen

Návrh zákona je předkládán zejména z důvodu zajištění řádné interpretace a aplikace právních předpisů, které obsahově navazují na zákon č. 181/2014 Sb., který má být nahrazen návrhem ZKB. Návrh zákona nemá ve vztahu k zákazu diskriminace žádné dopady. Co se týče rovnosti mužů a žen, návrh zákona je neutrální, neboť neobsahuje ustanovení, která by byť jen nepřímo zakládala rozdíly v právním postavení žen a mužů nebo v podmínkách vymáhání práv a plnění povinností.

3. Vysvětlení nezbytnosti navrhované právní úpravy v jejím celku

Návrh ZKB vyžaduje, aby byl předložen také změnový zákon, který zejména upraví rozsah povinností pro některé povinné osoby, které budou regulovány současně návrhem ZKB a těmi předpisy, jejichž změna je předkládána v rámci návrhu zákona.

Pokud jde o navrhovanou změnu ZEK, v případě jejího neprovedení by podnikatelům, kteří zajišťují veřejnou komunikační síť nebo poskytují veřejně dostupnou službu elektronických komunikací, při kybernetických bezpečnostních incidentech vznikala duplicitní povinnost spolupracovat jak s NÚKIB, tak také s ČTÚ, resp. by museli hlásit stejné informace zároveň na obě tato místa. Obdobně je tomu také v případě provozovatelů poštovních služeb podle zákona o poštovních službách. Takový právní stav by nutně vedl ke zbytečnému nárůstu administrativy na straně uvedených podnikatelů a ke zvýšení nákladů spojených právě s administrativními úkony.

V případě neprovedení navrhované změny ZoISVS by nastala situace, v níž by zmíněný právní předpis odkazoval na neexistující právní instituty a neexistující povinnosti dotčených osob. Došlo by tedy ke ztížení či znemožnění dosažení účelu právní úpravy ZoISVS. Vedle

toho by nepřijetí odkazu na bezpečnostní opatření podle návrhu zákona vedlo k nastavení trojkolejnosti právní úpravy kybernetické bezpečnosti v rámci veřejné správy v ČR.

Co se týče případného neprovedení úpravy ZoPZI, lze učinit tentýž závěr jako v případě neprovedení úpravy ZoISVS. Ustanovení ZoPZI by odkazovalo na neexistující okruh povinných osob, čímž by se stalo obsoletním.

Pokud jde o změny zvláštních zákonů upravujících povinnost mlčenlivosti a povinnost dodržet bankovní tajemství (ZoB, ZPMS, AML, daňový řád, ZCS, ZoPZI), jejich neprovedení by mělo za následek, že by příslušné subjekty nemohly z důvodu povinnosti mlčenlivost, resp. bankovního tajemství, poskytovat NÚKIB informace, které získaly při své činnosti či nezbytnou součinnost, jak je upraveno v návrhu ZKB.

4. Zhodnocení souladu navrhované právní úpravy s ústavním pořádkem ČR

Legitimita cíle, který sleduje návrh ZKB a s ním související návrh zákona, je v současnosti všeobecně považována za nezpochybnitelnou, neboť smyslem a účelem návrhu ZKB je pokračovat ve zvyšování bezpečnosti kybernetického prostoru a informací v něm.

Návrh změn v ZEK a zákoně o poštovních službách nestanovuje nové povinnosti, má pouze za úkol odstranit duplicitu povinností u subjektů, které by spadaly pod působnost obou zákonů zároveň, a přispívá tak k přehlednosti právní úpravy. Navrhované změny v ZoISVS mají zejména systematický charakter, neboť je vhodné přesunout všechny povinnosti související s regulací využívání cloud computingu orgány veřejné správy pod působnost jednoho zákona. V případě navrhovaných změn těchto tří právních předpisů nevzniká žádný rozpor s ústavním pořádkem ČR.

O navrhovaných změnách v ZoPZI lze také konstatovat, že jsou ústavně konformní. Již v případě účinného ZoPZI dochází k omezení práva podnikat, které ovšem obstojí vzhledem k legitimnímu cíli, jež omezení sleduje, totiž k ochraně bezpečnosti státu a vnitřního či veřejného pořádku. Navrhovaná změna pouze navíc odráží změny obsažené v návrhu ZKB, přičemž smysl původního znění ZoPZI zůstává plně zachován.

Také změny zvláštních zákonů upravujících povinnost mlčenlivosti a bankovní tajemství (ZoB, ZPMS, AML, daňový řád, ZCS, ZoPZI) je namístě považovat za ústavně konformní, neboť mají za cíl umožnit příslušným subjektům poskytovat NÚKIB informace či nezbytnou součinnost v rámci mechanismu prověřování rizik spojených s dodavatelem, který je upraven návrhem ZKB.

S ohledem na výše uvedené lze shrnout, že návrh zákona je plně v souladu s ústavním pořádkem ČR, jak jej vymezuje čl. 112 ústavního zákona č. 1/1993 Sb., Ústavy ČR, ve znění pozdějších předpisů (dále jen „Ústava“), jakož i s mezinárodními smlouvami podle čl. 10 Ústavy, a není v rozporu s nálezy Ústavního soudu.

5. Zhodnocení slučitelnosti navrhované právní úpravy s předpisy Evropské unie, judikaturou soudních orgánů Evropské unie nebo obecnými právními zásadami práva Evropské unie

Navrhovaný zákon je v souladu s předpisy Evropské unie (včetně směrnice NIS 2, transponované návrhem ZKB), judikaturou soudních orgánů Evropské unie a obecnými právními zásadami práva Evropské unie.

Přijetí návrhu změnového zákona je spolu s návrhem ZKB klíčovým nástrojem k implementaci směrnice NIS 2. Zhodnocení souladu navrhované právní úpravy s předpisy Evropské unie je důkladněji provedeno v důvodové zprávě k návrhu ZKB.

6. Zhodnocení souladu navrhované právní úpravy s mezinárodními smlouvami, kterými je ČR vázána, včetně zhodnocení slučitelnosti navrhované právní úpravy s mezinárodními smlouvami o lidských právech a základních svobodách

Navrhovaná úprava podstatným způsobem nezasahuje do mezinárodních smluv, kterými je ČR vázána, a je slučitelná s mezinárodními smlouvami o lidských právech a základních svobodách.

7. Předpokládaný hospodářský a finanční dopad navrhované právní úpravy na státní rozpočet, ostatní veřejné rozpočty a na podnikatelské prostředí ČR

7.1 Předpokládaný hospodářský a finanční dopad navrhované právní úpravy na státní rozpočet a ostatní veřejné rozpočty

V případě provedení změny ZEK a zákona o poštovních službách se nepředpokládají žádné zvýšené náklady. Ty by naopak přineslo neprovedení navrhovaných změn, neboť by státu vznikaly dvojnásobné náklady, pokud by docházelo ke zpracování totožných informací jak ze strany NÚKIB, tak ČTÚ.

Provedením změny ZoISVS, která je motivována záměrem zachovat kontinuitu dosavadní regulace, lze očekávat pouze minimální finanční dopad na státní rozpočet a ostatní veřejné rozpočty. Je namístě předpokládat, že obce s pověřeným obecním úřadem či obce I. stupně, kterým návrh zákona ukládá povinnost přiměřeně zavádět bezpečnostní opatření pro jejich informační systémy podle návrhu ZKB, již mají tato opatření zavedena z důvodu plnění původního požadavku ZoISVS.

Změnou ZoPZI by neměly vzniknout proti aktuálnímu stavu žádné zvýšené náklady.

Stejně tak v případě změn zvláštních zákonů upravujících povinnost mlčenlivosti a zachování bankovní tajemství (ZoB, ZPMS, AML, daňový řád, ZCS, ZoPZI) se proti aktuálnímu stavu nepředpokládají žádné zvýšené náklady.

Primárně budou veškeré výdaje a zvýšená potřeba v personální a platové oblasti, jež jsou spojeny s implementací návrhu zákona včetně prováděcích předpisů ve všech dotčených rozpočtových kapitolách, pokryty v rámci schválených rozpočtových limitů a stanovených limitů počtu míst a objemu prostředků na platy.

Pokud správci jednotlivých dotčených kapitol identifikují potřebu navýšení své kapitoly rozpočtu nad rámec schválených rozpočtových limitů nebo stanovených limitů počtu míst a objemu prostředků na platy, bude taková potřeba předmětem standardního vyjednávání o podobě relevantní kapitoly státního rozpočtu.

Nad rámec výše uvedeného je pro financování nákladů také možné využívat k tomu vzniklé nebo do budoucna vznikající dotační programy na úrovni Evropské unie, případně dotační programy původně na financování kybernetické bezpečnosti nezaměřené, ale dílčím způsobem k tomu využitelné (např. the Digital Europe Programme apod.).

7.2 Dopad na podnikatelské prostředí

Stejně jako v případě dopadů na státní rozpočet a ostatní veřejné rozpočty a územní dopady na územní samosprávné celky dochází pouze k minimálním dopadům z důvodu navrhované změny ZoISVS.Také v případě změny ZoPZI dochází pouze k minimálním dopadům na podnikatelské prostředí. Změna zákona o prověřování zahraničních investic následuje analogicky původní rozvržení tzv. cílových osob, a tedy v případě dopadů na podnikatelské prostředí je možné odkázat na řešení této otázky v důvodové zprávě k ZoPZI.

. Na druhé straně lze v případě provedení navrhované změny ZEK a zákona o poštovních službách jako pozitivní vnímat zamezení stavu spočívajícího ve zvýšené administrativní zátěži podnikatelů zajišťujících veřejnou komunikační síť nebo poskytujících veřejně dostupnou službu elektronických komunikací, stejně tak jako poskytovatelů poštovních služeb, která by v případě neprovedení změny vznikala při snaze vyhovět duplicitním povinnostem podle návrhu ZKB a ZEK, resp. zákona o poštovních službách.

V případě změn zvláštních zákonů upravujících povinnost mlčenlivosti a povinnost dodržet bankovní tajemství (ZoB, ZPMS, AML, daňový řád, ZCS, ZoPZI) není namístě očekávat jakékoliv dopady na podnikatelské prostředí.

8. Zhodnocení sociálních dopadů, včetně dopadů na specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny, dopadů na ochranu práv dětí a dopadů na životní prostředí

8.1 Sociální dopady, včetně dopadů na rodiny a dopadů na specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny

Návrh zákona nemá žádné dopady na rodiny a specifické skupiny obyvatel, zejména osoby sociálně slabé, osoby se zdravotním postižením a národnostní menšiny.

8.2 Dopady na ochranu práv dětí

Návrh zákona nemá žádné dopady na ochranu práv dětí.

8.3 Dopady na životní prostředí

Návrh zákona nemá žádné dopady na životní prostředí.

9. Zhodnocení dopadů navrhovaného řešení ve vztahu k ochraně soukromí a osobních údajů

Návrh zákona nemá žádný negativní dopad na ochranu soukromí a osobních údajů, posouzení nezbytnosti a přiměřenosti zpracování, souvisejících rizik pro práva a svobody fyzických osob, a stanovení možných opatření ke snížení těchto rizik tak není v tomto případě relevantní.

10. Zhodnocení korupčních rizik

Vzhledem k povaze navrhovaných změn ZEK, ZoISVS a zákona o poštovních službách nepřináší návrh zákona zvýšení korupčních rizik v porovnání se stávající úpravou. Stejný závěr platí také pro změny zvláštních zákonů upravujících povinnost mlčenlivosti a povinnost dodržet bankovní tajemství (ZoB, ZPMS, AML, daňový řád, ZCS, ZoPZI).

Korupční rizika spojená se změnou ZoPZI zůstávají stejná, lišit se může pouze jejich četnost v návaznosti na očekávané zvýšení počtu cílových osob, u kterých bude potřeba získat povolení nebo podmíněné povolení pro uskutečnění investice.

11. Zhodnocení dopadů na bezpečnost nebo obranu státu

Navrhovaná úprava nemá zásadní vliv na bezpečnost nebo obranu státu. Tento vliv se odvíjí od návrhu ZKB a společně s návrhem zákona přispívají k vyšší bezpečnosti a obraně státu.

12. Zhodnocení dopadů na rodiny

Návrh zákona nemá žádné dopady na rodiny.

13. Zhodnocení územních dopadů, včetně dopadů na územní samosprávné celky

Návrh zákona nemá žádné územní dopady, včetně dopadů na územní samosprávné celky.

14. Zhodnocení souladu navrhovaného řešení se zásadami tvorby digitálně přívětivé legislativy, včetně zhodnocení rizika vyloučení nebo omezení možnosti přístupu specifických skupin osob k některým službám v důsledku digitalizace jejich poskytování (digitální vyloučení)

Z hlediska zásad tvorby digitálně přívětivé legislativy jsou respektovány zásady budování přednostně digitálních služeb a maximální opakovatelnosti a znovupoužitelnosti údajů. Zamýšleným zrušením duplicity povinností ukládaných podle návrhu ZKB a ZEK, resp. zákona o poštovních službách (v případě navrhovaných změn posledních dvou jmenovaných) a povinností ukládaných podle zákona o ochraně utajovaných informací. Výrazně tak bude usnadněno budování digitálních služeb, zamýšlené úpravy jsou zároveň jednoznačně postaveny na principu *only once*, jehož charakteristickým znakem je, že zamezuje případům, kdy konkrétní osoby předkládají orgánům veřejné správy tytéž informace opakovaně.

B. Zvláštní část

K části první – změna zákona o bankách

Návrh zákona v této části reaguje na povinnost poskytovat nezbytnou součinnost při prověřování rizik spojených s dodavatelem upravenou v § 28 odst. 4 návrhu ZKB. V ZoB je návrhem rozšířen taxativní výčet případů, kdy banka vydává zprávu o záležitostech, které jsou předmětem bankovního tajemství.

K části druhé – změna zákona o poštovních službách

K bodu 1

Navrhuje se nad rámec stávajících povinností držitele poštovní licence posílit požadavek na bezpečnost poštovní sítě, základních služeb a přístupu k poštovní infrastruktuře tak, že se nad rámec souvisejících stávajících povinností (zejména podle stávajícího odstavce 2, 3 a 8 předmětného ustanovení) doplňuje povinnost hlásit bezpečnostní incidenty, resp. ohrožení nebo narušení bezpečnosti sítě, základních služeb nebo poskytování základních služeb nebo přístupu k poštovní infrastruktuře. S ohledem na skutečnost, že poskytovatelé poštovních služeb mají nově podle směrnice NIS 2 podléhat této směrnici, resp. regulaci oblasti kybernetické bezpečnosti v ní obsažené, je rovněž potřeba jednoznačně nastavit rozdělení kompetencí mezi ČTÚ a NÚKIB. Takové jednoznačného rozdělení kompetencí je důležité i z důvodu požadavku na nezvyšování administrativní zátěže jak na straně povinného, tak na straně ČTÚ, resp. NÚKIB. Díky navrhované změně by nemělo docházet k duplicitnímu plnění povinnosti hlásit bezpečnostní incidenty vůči oběma těmto orgánům, a naopak by tyto incidenty měly být oznamovány pouze jednou.

K bodu 2 až 4

Úprava odkazu v důsledku přečíslování odstavců podle bodu 1.

K bodu 5

Obdobně jako v případě § 112a ZEK se navrhuje doplnit úprava spolupráce ČTÚ s NÚKIB.

K bodu 6

Navrhuje se doplnit skutková podstata přestupku za porušení nově stanovené informační povinnosti držitele poštovní licence podle bodu 1 hlásit bezpečnostní incidenty ČTÚ.

K bodu 7, 8 a 11

Úprava odkazu v důsledku přečíslování odstavců podle bodu 1.

K bodu 9 a 10

Navrhuje se doplnit sankce za spáchání doplněného přestupku podle bodu 6.

K části třetí – změna zákona o informačních systémech veřejné správy

Vzhledem k tomu, že návrh ZKB nestanoví na rozdíl od zákona č. 181/2014 Sb. pro orgány veřejné moci povinnost zajistit dodržování bezpečnostních pravidel pro orgány veřejné moci využívající služby cloud computingu ani povinnost zařadit poptávaný cloud computing do bezpečnostní úrovně před uzavřením smlouvy s poskytovatelem cloud computingu, a vzhledem k tomu, že je návrhem ZKB rušen prováděcí právní předpis stanovující tato bezpečnostní pravidla, je nutné promítnout do zákona č. 365/2000 Sb., o informačních systémech veřejné správy, důsledky z těchto změn plynoucí.

K bodu 1

Navrhuje se upravit definice bezpečnostní úrovně informačního systému veřejné správy, aby povinnost orgánu veřejné správy vyjádřena v § 6n měla oporu v tomto definičním ustanovení. Kybernetickým bezpečnostním incidentem se rozumí kybernetický bezpečnostní incident podle zákona o kybernetické bezpečnosti.

K bodu 2

Navrhuje se doplnit definice bezpečnostních pravidel pro orgány veřejné správy využívající služby poskytovatelů cloud computingu, aby povinnost orgánu veřejné správy vyjádřena v § 6l odst. 3 měla oporu v tomto definičním ustanovení.

K bodům 3, 6 a 7

Navrhuje se přenést (resp. zachovat v případě bezpečnostních pravidel pro orgány veřejné správy využívající služby cloud computingu) pravomoc kontrolovat požadavky přímo související s kybernetickou bezpečností na NÚKIB jakožto garanta kybernetické bezpečnosti v ČR. Agentuře zůstane zachována pravomoc kontrolovat splnění požadavku podle § 6n písm. a), protože tento se týká informační koncepce ČR, a nesouvisí tak přímo s kybernetickou bezpečností. Navrhovaná ustanovení rovněž reflektují přesun zmocnění k vydání vyhlášky o bezpečnostních úrovních a bezpečnostních pravidlech ze zákona č. 181/2014 Sb. do ZoISVS s cílem sjednotit úpravu cloud computingu v jednom předpisu.

Při výkonu kontrolní pravomoci podle navrhovaného ustanovení postupují pověření zaměstnanci NÚKIB podle zákona č. 255/2012 Sb., o kontrole (kontrolní řád), ve znění pozdějších předpisů.

K bodům 4 a 5

V návaznosti na navrhovanou změnu věty druhé § 5a a § 5b je potřeba uvést, že zákon č. 181/2014 Sb. upravoval práva a povinnosti malé skupiny povinných osob. Směrnice NIS 2 přichází s mnohem plošnějším přístupem, a návrh ZKB tak reguluje širší skupinu povinných osob. ZoISVS v sobě obsahuje požadavky na kybernetickou bezpečnost informačních systémů veřejné správy, protože tyto požadavky nebyly součástí ambice původní úpravy zákona č. 181/2014 Sb. Návrh ZKB již nepracuje pouze s jednou úrovní bezpečnostních opatření (s úpravami pro významné informační systémy) pro nejvýznamnější subjekty v ČR a přichází s úpravou bezpečnostních opatření pro širokou skupinu subjektů v ČR, konkrétně bezpečnostními opatřeními pro režim nižších povinností.

Rovněž je vhodné v rámci státu stanovit pravidla kybernetické bezpečnosti shodným způsobem, ať již z hlediska možného rozšíření poskytovatelů regulovaných služeb směrem k dalším správcům informačních systémů veřejné správy v budoucnu, či vzhledem ke sdílení zkušeností a lidských zdrojů. Z těchto důvodů došlo po konzultaci se zástupci Ministerstva vnitra a Digitální informační agentury k zařazení tohoto ustanovení a přechodu úpravy bezpečnostních opatření do návrhu ZKB.

Povinnost zavádět bezpečnostní opatření je pak stanovena tak, že správci informačních systémů veřejné správy zavádějí bezpečnostní opatření, obsažená ve vyhlášce týkající se poskytovatele regulované služby v režimu nižších povinností, přiměřeně. Přiměřenost odkazuje ke dvěma aspektům této úpravy. První z nich je nákladová přiměřenost zaváděných opatření, která je tímto, vzhledem k velikosti a významnosti adresátů této normy, akcentována, a která byla vůdčím principem zavádění bezpečnostních opatření i v rámci původní úpravy. Jde o princip, který vyjadřuje, že opatření jsou zaváděna v takové úrovni a míře, která odpovídá nákladům na pořízení těchto opatření, které by neměly převýšit náklady dopadu narušení bezpečnosti informací v rámci daných aktiv. Správce přihlíží zejména k možným dopadům

narušení důvěrnosti, integrity a dostupnosti konkrétního informačního systému veřejné správy na svou běžnou činnost a na poskytování svých služeb občanům. Zjednodušeně řečeno, čím důležitější je informační systém veřejné správy pro řádné fungování jeho správce, tím více prostředků je vhodné vynaložit na jeho zabezpečení. Přiměřené zavádění bezpečnostních opatření lze chápat také tak, že správce nezavádí všechna opatření, na která toto ustanovení odkazuje, ale pouze ta, která jsou pro konkrétní informační systém veřejné správy proveditelná a vhodná.

Druhým aspektem přiměřenosti je pak zohlednění toho, že správců informačních systémů veřejné správy se týkají pouze požadavky na zajišťování bezpečnosti prostřednictvím zavádění bezpečnostních opatření, a nevztahují se na ně další požadavky dané návrhem ZKB, tedy např. nemají povinnost hlásit kybernetické bezpečnostní incidenty. Z toho důvodu se na ně nevztahuje pasáž vyhlášky, která se týká vyhodnocování významnosti incidentu za účelem posouzení, zda je nutné tento incident nahlásit.

K bodu 5

Navrhovaná změna reaguje na odlišné pojetí povinných osob v návrhu ZKB. Ten stanoví pouze jedinou povinnou osobu, kterou je poskytovatel regulované služby. Je tedy potřeba změnit ustanovení stanovující kontrolní oprávnění pro NÚKIB ke kontrole dodržování některých povinností vyplývajících ze ZoISVS tak, aby byl odkaz na regulované systémy podle zákona č. 181/2014 Sb. nahrazen odkazem na regulované služby, resp. poskytování regulovaných služeb podle návrhu ZKB.

K bodům 8, 15 a 16

Návrh ZKB na rozdíl od zákona č. 181/2014 Sb. již nestanoví povinnost zařadit poptávaný cloud computing do bezpečnostní úrovně a zajistit, že budou dodržována bezpečnostní pravidla, a ani neobsahuje zmocnění k vydání prováděcích právních předpisů pro stanovení bezpečnostních úrovní pro využívání cloud computingu orgány veřejné moci a pro stanovení bezpečnostních pravidel. Proto je k zachování funkčnosti systému regulace využívání cloud computingu orgány veřejné správy nutné tyto povinnosti (a s nimi i prováděcí právní předpisy) přenést do ZoISVS, který právě těžiště regulace využívání cloud computingu orgány veřejné správy obsahuje. Navrhovanými změnami se tedy přenáší povinnost pro orgány veřejné moci zařadit informační systém, jehož provoz má být zajištěn cloud computingem, do bezpečnostní úrovně podle prováděcího právního předpisu, stejně jako povinnost zajistit po celou dobu využívání služeb cloud computingu dodržování bezpečnostních pravidel podle prováděcího právního předpisu. Zmocnění k vydání těchto prováděcích právních předpisů zůstává NÚKIB, rovněž se ale přesouvá do ZoISVS.

K bodu 9

Navrhuje se změna v textu, která zohlední přesun vyhlášky o bezpečnostních pravidlech pod ZoISVS, včetně formulace primární povinnosti orgánu veřejné moci obsažené v § 4 odst. 5 zákona č. 181/2014 Sb., a která povede ke zpřesnění požadavku obsaženého v § 6n písm. c).

K bodu 10

Další předkládanou změnou ZoISVS je napravení rozporu legislativního textu s faktickým stavem, kdy v novelizačním textu vyjmenovaná ustanovení předpokládala stanovení některých náležitostí žádosti o zápis do katalogu cloud computingu právním předpisem upravujícím kybernetickou bezpečnost, avšak tyto náležitosti jsou stanoveny prováděcím právním předpisem vydaným podle zákona o informačních systémech veřejné správy.

K bodům 11 a 12

Navrhovaná úprava doplňuje přestupky za porušení povinností již stanovených ZoISVS nebo zákonem č. 181/2014 Sb. (odstavec 4 písm. d), orgány veřejné moci nebo poskytovateli cloud computingu.

Cílem navrhované úpravy je zajistit vynutitelnost těchto povinností a tím odstranit nedostatek spočívající v imperfekci ZoISVS. Navrhovaná úprava tak nově zakotvuje přestupky v návaznosti na porušení povinnosti poskytovatele cloud computingu týkající se řádného poskytování cloud computingu nebo orgánu veřejné správy týkající se využívání cloud computingu, ukončení jeho využívání v případě, že cloud computing přestane splňovat zákonné požadavky na něj kladené, zařazení informačního systému veřejné správy do bezpečnostní úrovně a zajištění dodržení bezpečnostních pravidel. Navazující úprava sankcí zároveň bude na povinné subjekty působit dostatečně motivačně, aby se přestupkového jednání nedopouštěly.

K bodu 13

S cílem zachovat donucovací charakter pokuty se navrhuje doplnit její novou výši, která bude lépe odpovídat finančním možnostem poskytovatelů cloud computingu a hodnotě uzavíraných kontraktů na poskytování služeb cloud computingu.

Zároveň navrhovaná výše sankce u přestupků podle odst. 5 odpovídá současnému nastavení sankce za přestupek podle § 25 odst. 3 písm. c), odst. 4 písm. c), odst. 5 písm. c), odst. 6 písm. c), odst. 7 písm. c), odst. 8) a odst. 9 písm. a) zákona č. 181/2014 Sb. Ten považuje nezařazení do bezpečnostní úrovně a nezajištění dodržování bezpečnostních pravidel orgány veřejné moci za středně závažný přestupek. Její výše byla nastavena s ohledem na zvyšování sankcí v novém návrhu zákona o kybernetické bezpečnosti v důsledku požadavků směrnice NIS 2 na nastavení účinných sankcí.

K bodu 14

Navrhuje se upravit rovněž § 9e, který odkazuje v případě likvidace dat na úpravu týkající se významných informačních systémů, přičemž tato povinná osoba již v návrhu ZKB neexistuje. Vzhledem k existenci pouze jedné povinné osoby a jediné úpravy likvidace dat postačuje navrhovaná podoba odkazu.

K části čtvrté – změna zákona o elektronických komunikacích

K bodu 1 až 3

V návaznosti na návrh ZKB byl ze strany ČTÚ identifikován možný problém při výstavbě a rozvoji sítí elektronických komunikacích, které v rámci své regulační činnosti podporuje, a to zejména stran nových povinností spojených s dodavatelským řetězcem. Konkrétně ČTÚ spatřuje riziko ve fázi intenzivní výstavby nebo rozvoje sítí elektronických komunikací.

Například mobilních 5G sítí, pokud by byl držitel přídělu rádiových kmitočtů podle § 22 ZEK zasažen v důsledku protiopatření nebo opatření obecné povahy vydaného podle § 31 odst. 1 návrhu ZKB vynucenou změnou dodavatele technologie, prostřednictvím které naplňuje povinnosti a podmínky stanovené v přídělu rádiových kmitočtů, včetně závazků, které držitel přídělu převzal v průběhu výběrového řízení na udělení práva k využívání rádiových kmitočtů. To může způsobit nemožnost splnit podmínky a povinnosti uložené v příslušném rozhodnutí vydaném ČTÚ. Navrhuje se proto v § 22a ZEK doplnit, aby předseda Rady ČTÚ mohl rozhodnout o změně již uděleného přídělu radiových kmitočtů, pokud by to bylo nezbytné pro plnění protiopatření nebo plnění účelu opatření obecné povahy vydaného podle návrhu ZKB.

Vzhledem k tomu, že se tento problém může potenciálně dotýkat nikoli pouze oblasti regulace rádiového spektra, ale i dalších regulovaných oblastí upravených ZEK obecně, tj. jakéhokoli regulačního rozhodnutí vydávaného ČTÚ, navrhuje se doplnění ZEK o obecné pravidlo stanovené v navrhovaném § 6 odst. 6 ZEK v rámci regulačních zásad. Toto ustanovení umožňuje ČTÚ rozhodnout o změně nebo zrušení regulačního opatření uloženého na základě ZEK, pokud plnění podmínek v něm stanovených znemožňuje nebo brání podmínky uvedené v protiopatření nebo opatření obecné povahy, jež byly vydány na základě návrhu ZKB.

K bodu 4

V rámci svého čl. 43 ruší směrnice NIS 2 k datu nabytí své účinnosti čl. 40 a 41 směrnice Evropského parlamentu a Rady (EU) 2018/1972 ze dne 11. prosince 2018, kterou se stanoví evropský kodex pro elektronické komunikace (dále jen „Kodex“). Je tomu tak zjednodušeně z toho důvodu, že dosavadní požadavky Kodexu, tedy *„zajistit, aby poskytovatelé veřejných sítí elektronických komunikací nebo veřejně dostupných služeb elektronických komunikací přijali vhodná a přiměřená technická a organizační opatření k odpovídajícímu zvládnutí rizik pro bezpečnost sítí a služeb. […]“*, odpovídají požadavkům směrnice NIS 2, která technická a organizační opatření všem poskytovatelům veřejných sítí elektronických komunikací a veřejně dostupných služeb elektronických komunikací také ukládá.

Transpozičním ustanovením článků 40 a 41 Kodexu je v českém právním prostředí § 98 ZEK, ve znění novelizace provedené zákonem č. 374/2021 Sb., účinné od 1. ledna 2022.

Ustanovení § 98 ZEK doznalo touto novelizací změn a vztahuje se na *„osoby zajišťující veřejnou komunikační síť nebo poskytující veřejně dostupnou službu elektronických komunikací […]“*, tedy na širší množinu, než na kterou dopadá návrh ZKB. Z výše uvedených důvodů, a z důvodu minimalizace zásahu do jiných právních předpisů, doplňuje návrh zákona aktuální znění ZEK o nový odstavec upravující vztah povinných osob podle ZEK a návrhu ZKB. Návrh ZKB je v této úzké problematice zvláštním předpisem vůči ZEK.

Nový odstavec tak stanovuje, že vyjmenované odstavce § 98 ZEK, které stanovují pro podnikatele zajišťující veřejnou komunikační síť nebo poskytujícího veřejně dostupnou službu elektronických komunikací nějaké povinnosti, se v daném případě nepoužijí. *A contrario* tedy platí, že se pravidla obsažená v návrhu ZKB uplatní pouze v případě, že k narušení bezpečnosti a integrity veřejných sítí a veřejně dostupných služeb došlo v kyberprostoru. Za splnění tohoto předpokladu se v případě obdobné povinnosti stanovené návrhem ZKB neuplatní povinnosti stanovené v uvedených odstavcích § 98 ZEK nebo uložené ČTÚ na jejich základě. Pokud v návrhu ZKB obdobná povinnost neexistuje, uplatní se povinnosti stanovené v § 98 ZEK nebo uložené ČTÚ na jejich základě. Zbylá ustanovení ZEK a povinnosti plynoucí těmto orgánům nebo osobám z těchto ustanovení nejsou dotčena.

K části páté – změna zákona o provádění mezinárodní sankcí

Institut mlčenlivosti podle ZPMS chrání všechny úkony učiněné podle tohoto zákona a informace získané při jeho provádění, neboť se velmi často jedná o citlivé informace, jejichž únik na veřejnost by mohl vést k ohrožení konkrétních osob, veřejného zájmu či bezpečnosti ČR. Absolutní mlčenlivost je prolomena pouze taxativním výčtem výluk obsahující konkrétní orgán a konkrétní účel prolomení. Tento taxativní výčet je však postupně rozšiřován, nyní opět v reakci na § 28 odst. 3 návrhu ZKB, a dosahuje původně nepředpokládaných rozměrů. Vzhledem k tomuto rozšiřování je nezbytné přijmout pojistku po vzoru § 39 odst. 4 AML, aby byl zachován původní účel institutu mlčenlivosti podle ZPMS.

Současně s novou výlukou z povinnosti mlčenlivosti je tak do ZPMS doplněn § 16 odst. 7, který má za cíl zajistit ochranu práv a oprávněných zájmů osob, stejně jako veřejného zájmu a bezpečnosti ČR, a to prostřednictvím jednak redukce poskytovaných informací na nezbytně

nutný rozsah vzhledem k účelu poskytnutí, jednak neuplatnění výluky v případě ohrožení či zmaření šetření Finančního analytického úřadu či probíhajícího trestního řízení či v případě zjevné nepřiměřenosti oprávněným zájmům osoby nebo účelu poskytnutí.

K části šesté – změna zákona o některých opatřeních proti legalizaci výnosů z trestné činnosti a financování terorismu

Obdobně jako v případě změny ZPMS dochází v AML k rozšíření taxativního výčtu výluk z mlčenlivosti v § 39 odst. 1, a to v reakci na povinnost Finančního analytického úřadu poskytovat informace podle § 28 odst. 3 návrhu ZKB.

K části sedmé – změna daňového řádu

Dochází k rozšíření taxativního výčtu výluk z mlčenlivosti doplněním písm. n) do § 53 odst. 1, a to v reakci na obecnou povinnost poskytovat nezbytnou součinnost podle § 28 odst. 4 návrhu ZKB.

K části osmé – změna zákona o Celní správě České republiky

Dochází k rozšíření taxativního výčtu výluk z mlčenlivosti v § 27 odst. 3, a to v reakci na obecnou povinnost poskytovat nezbytnou součinnost podle § 28 odst. 4 návrhu ZKB.

K části deváté – změna zákona o prověřování zahraničních investic

K bodu 1

Návrh změny ZoPZI následuje analogicky původní rozvržení tzv. cílových osob. Snahou stanovení jednoho z okruhů cílových osob jako poskytovatelů regulované služby v režimu vyšších povinností podle návrhu ZKB je přiblížit se v prostředí nového rozvržení kategorií povinných osob podle návrhu ZKB původnímu úmyslu dosavadního znění ZoPZI.

K bodu 2

Je navrhováno nové ustanovení, které představuje výjimku z povinnosti zachovávat mlčenlivost podle § 20 ZoPZI a vztahuje se na zaměstnance Ministerstva průmyslu a obchodu pověřené řízením nebo konzultací podle ZoPZI. V rámci spolupráce Ministerstva průmyslu a obchodu s NÚKIB při pověřování bezpečnosti dodavatelského řetězce se tato povinnost tudíž neuplatní. Tato změna reflektuje úpravu spolupráce obsaženou v § 28 odst. 1 návrhu ZKB, podle níž Ministerstvo průmyslu a obchodu, za účelem shromažďování a vyhodnocování informací a dat podle § 27 odst. 1 návrhu ZKB, poskytne NÚKIB na jeho žádost bez zbytečného odkladu, nejpozději do 30 dnů ode dne obdržení žádosti, stanovisko o rizikovosti dodavatele nebo informace, které získalo při své činnosti.

K části desáté – účinnost

Protože podstatnou část návrhu ZKB, a tedy i návrhu zákona, tvoří transpozice směrnice NIS 2, je s požadavky této směrnice úzce spojeno také stanovení účinnosti nové právní úpravy. V souladu s obsahem čl. 41 odst. 1 jsou členské státy povinny přijmout a zveřejnit opatření nezbytná pro dosažení souladu s uvedenou směrnicí do 17. října 2024, tato opatření se použijí od 18. října 2024. Vzhledem k tomu, že zde existuje naléhavý obecný zájem, spočívající v nutnosti implementace směrnice NIS 2 do určeného termínu, lze podle § 3 odst. 4 zákona č. 309/1999 Sb., o Sbírce zákonů a o Sbírce mezinárodních smluv, ve znění pozdějších předpisů, stanovit dřívější den nabytí účinnosti, než který je stanovený v odst. 3 tohoto ustanovení, tedy k 1. lednu nebo k 1. červenci kalendářního roku, nejdříve však počátkem dne následujícího po dni vyhlášení právního předpisu. V případě, že by nebyla směrnice NIS 2 implementována v řádném termínu, může Evropská komise zahájit s Českou republikou řízení o nesplnění povinnost podle čl. 258 a násl. Smlouvy o fungování EU. Z tohoto důvodu je nutné, aby byla právní úprava podle tohoto návrhu zákona a jeho prováděcích právních předpisů přijata nejpozději k 18. říjnu 2024 a zároveň ještě předtím byla zajištěná dostatečná legisvakanční lhůta, aby se povinné orgány a osoby stihly připravit na veškeré povinnosti.

V Praze dne 17. července 2024

Předseda vlády:

prof. PhDr. Petr Fiala, Ph.D., LL.M.

podepsáno elektronicky

Elektronický podpis: 22.7.2024
Certifikát autora podpisu:
Jméno: Ing. Lukáš Kintr
Vydal: I.CA EU Qualified CA2/RSA 06/2022
Platnost do: 10.12.2024 14:03 +01:00

Ředitel Národního úřadu pro kybernetickou a informační bezpečnost:

Ing. Lukáš Kintr

podepsáno elektronicky

Digitálně podepsal
Petr Fiala
24. 7. 2024