|  |
| --- |
| **TABUĽKA  ZHODY**právneho predpisu s právom Európskej únie |
| Smernica Európskeho parlamentu a Rady 2002/58/ES z  12. júla 2002, týkajúca sa spracovávania osobných údajov a ochrany súkromia v sektore elektronických komunikácií (smernica o súkromí a elektronických komunikáciách) (Ú. v. ES L 201, 31.7.2002; Mimoriadne vydanie Ú. v. EÚ, kap. 13/zv. 29) v platnom znení. | Právne predpisy Slovenskej republikyNávrh zákona, ktorým sa mení a dopĺňa zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov a ktorým sa menia a dopĺňajú niektoré zákony |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| Článok(Č, O, V, P) | Text | Spôsob transpozície (N, O, D, n.a.) | Číslo predpisu | Článok(Č, §, O, V, P) | Text | Zhoda | Poznámky | Identifikácia goldplatingu | Identifikácia oblasti goldplatingu a vyjadrenie k opodstatnenosti goldplatingu\* |
| **Č:4** | **Bezpečnosť spracovania** |  |  |  |  |  |  |  |  |
| Č:4, O:1 | Poskytovateľ verejne dostupnej elektronickej komunikačnej služby musí uskutočniť vhodné technické a organizačné opatrenia na zaručenie bezpečnosti svojej služby, ak je to z hľadiska bezpečnosti siete nevyhnutné aj v spojení s poskytovateľom verejnej komunikačnej siete. So zreteľom na stav techniky a náklady na ich implementáciu, tieto opatrenia musia zaručiť úroveň bezpečnosti primeranú existujúcemu riziku. | N | Návrh zákona | § 19O:1 | Prevádzkovateľ základnej služby je povinný do 12 mesiacov odo dňa zápisu do registra prevádzkovateľov základnej služby v závislosti od vykonanej analýzy rizík prijať, dodržiavať a vykonávať všeobecné bezpečnostné opatrenia najmenej v rozsahu bezpečnostných opatrení podľa § 20 a vykonávať ich s cieľom zabezpečovania kybernetickej bezpečnosti a odolnosti. Na účely plnenia povinnosti podľa prvej vety prevádzkovateľ základnej služby prijíma, dodržiava a vykonáva sektorové bezpečnostné opatrenia, ak sú ustanovené; 24) povinnosť prijímať opatrenia podľa § 20 ods. 4 tým nie je dotknutá. Osoba poskytujúca niektorú zo služieb alebo vykonávajúcu niektorú z činností podľa § 2 ods. 3 plní bezpečnostné opatrenia podľa osobitného predpisu.24a)Poznámky pod čiarou k odkazom 24 a 24a znejú:24) Napríklad nariadenie Európskeho parlamentu a Rady (EÚ) 2022/2554 zo 14. decembra 2022 o digitálnej prevádzkovej odolnosti finančného sektora a o zmene nariadení (ES) č. 1060/2009, (EÚ) č. 648/2012, (EÚ) č. 600/2014, (EÚ) č. 909/2014 a (EÚ) 2016/1011 (Ú. v. EÚ L 333, 27.12.2022), zákon č. 541/2004 Z. z., zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, vyhláška Úradu jadrového dozoru Slovenskej republiky č. 430/2011 Z. z. o požiadavkách na jadrovú bezpečnosť v znení vyhlášky č. 103/2016 Z. z.24a) Vykonávacie nariadenie Komisie (EÚ) ..../... z .... ..., ktorým sa stanovujú pravidlá pre uplatňovanie smernice (EÚ) 2022/2555, pokiaľ ide o technické a metodologické požiadavky na opatrenia na riadenie rizík v oblasti kybernetickej bezpečnosti a ďalšie špecifikácie prípadov, v ktorých sa incident považuje za významný s ohľadom na poskytovateľov služieb DNS, registre TLD, poskytovateľov cloudových služieb, poskytovateľov služieb dátových centier, poskytovateľov sietí na doručovanie obsahu, poskytovateľov riadených služieb, poskytovateľov riadených bezpečnostných služieb, poskytovateľov online trhovísk, online vyhľadávačov a platforiem sociálnych sietí a poskytovateľov dôveryhodných služieb. | Ú | Ustanovenie je implementované tým, že všetci poskytovatelia verejne dostupnej elektronickej komunikačnej siete podliehajú regulácii upravenej zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti | GP-N |  |
| Č:4, O:2 | V prípade osobitného rizika narušenia bezpečnosti siete, poskytovateľ verejne dostupnej elektronickej komunikačnej služby musí informovať príslušných účastníkov o takom riziku a ak je riziko mimo rozsahu platnosti opatrení, ktoré má uskutočniť poskytovateľ služby, o akýchkoľvek možných nápravných prostriedkoch, vrátane údajov o predpokladaných vyvolaných nákladoch. | N | Návrh zákona | §: 1P:a | S cieľom zaistiť kybernetickú bezpečnosť a zabezpečiť efektívne riešenie kybernetických bezpečnostných incidentov tento zákon upravuje 1. podmienky pre riadenie a zabezpečenie kybernetickej bezpečnosti, najmä
	1. postavenie a povinnosti prevádzkovateľa základnej služby,
	2. bezpečnostné opatrenia,
	3. hlásenie kybernetického bezpečnostného incidentu, významnej kybernetickej hrozby, udalosti odvrátenej v poslednej chvíli a zraniteľnosti,
	4. riešenie kybernetického bezpečnostného incidentu,
	5. opatrenia proti produktom IKT, službám IKT alebo procesom IKT ohrozujúcim kybernetickú bezpečnosť a proti škodlivému obsahu,
 | Ú | Ustanovenie je implementované tým, že všetci poskytovatelia verejne dostupnej elektronickej komunikačnej siete podliehajú regulácii upravenej zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti. | GP-N |  |