**Ďalšie predložené podnety a pripomienky k súčasnému zákonu č. 289/2008 Z. z. o používaní elektronickej registračnej pokladnice a v znení neskorších predpisov a návrhy na zmeny v novom zákone o používaní pokladnice e-kasa klient**

***SAPFiZ (SLOVENSKÁ ASOCIÁCIA PREDAJCOV FIŠKÁLNYCH ZARIADENÍ)***

*Všeobecne k platnému zákonu*

Slovenska republika ma dlhoročnú tradíciu s používaním fiškálnych zariadení, ktorá siaha až do roku 1994. V súčasnosti platný zákon 289/2008 prijatý v roku 2008, bol od svojho prijatia viac ako 13x novelizovaný. To znamená, že MFSR a Finančná sprava na základe zistení z praxe, postupne upresňovala znenia zákona tak, aby sa zákon stal efektívnym nástrojom eliminácie daňových únikov.

Považujeme za nutné pokračovať v zlepšovaní toho čo sa roky vybudovalo na základe súčasných poznatkov MFSR i Finančnej správy SR i čerpať zo skúsenosti a smerovania v iných tradičných fiškálnych krajinách (Taliansko, Poľsko, Rumunsko, Maďarsko, Nemecko, Grécko, Rakúsko, Rusko, Švédsko ...). Je preukázateľne, že v týchto krajinách je jednoznačne identifikovateľný trend zvyšovania bezpečnostných štandardov ochrany fiškálnych údajov uložených vo fiškálnych zariadeniach a ich následne odosielanie na servera finančnej správy pre potreby ich následného spracovania.

Pripojenie fiškálnych zariadení online na servery FS je preto krok MFSR a FS správnym smerom. Je však nevyhnutne venovať patričnú pozornosť zvyšovaniu bezpečnostných štandardov ochrany fiškálnych údajov vo fiškálnych zariadeniach na ktorých fiškálne údaje vznikajú. Bezpečne uložené fiškálne údaje vo fiškálnych zariadeniach a ich fyzická kopia na serveroch FS je základný kameň moderných fiškálnych legislatív v tradičných fiškálnych krajinách.

V rámci pripomienkovania boli autori predloženého návrhu zákona upozorňovaní aj zo strany APZD, že súčasná verzia zákona obsahuje viacero zásadných nedostatkov, nepresností a nedorozumení, ktoré je potrebné upraviť tak, aby táto novela dokázala skutočne naplniť očakávania správcu dane v oblasti lepšieho výberu daní.

Bohužiaľ neúspešne. Súčasná prax potvrdzuje, že naše pripomienky boli a sú opodstatnené. Vybrané opatrenia, ktoré navrhujeme opätovne zapracovať do súčasného zákona, paradoxne v zákone o používaní registračných pokladníc boli pred jeho novelou v roku 2018, no novela ich zrušila bez adekvátnej náhrady. Zrušenie týchto opatrení zvyšuje v podstatnej miere riziko vzniku daňových únikov.

Problematika je pomerne rozsiahla a odborná, preto v predmetnej úprave zákona veľmi záleží na detailoch riešenia, aj paragrafového znenia. Navrhujeme overené riešenia, ktoré používajú najvyspelejšie systémy kontroly daní, prostredníctvom ktorých by sme chceli významne zvýšiť kvalitu a bezpečnosť systému na svetovú úroveň poznatkov v tejto oblasti s dodržaním zásad.

1.1 On-line je výborným bezpečnostným doplnkom existujúcich fiškálnych zariadení

1.2 Údaje ukladané v zabezpečenom elektronickom žurnále v zabezpečenom dátovom úložisku už počas vytvárania účtenky

1.3 Zabezpečené dátové úložisko musí chrániť dáta šifrovaním predpísaným spôsobom, aj zamedzením manipulácie s úložiskom plombovaním zariadenia registrovanou daňovou plombou

1.4 Je nutné doplniť, aby správne zabezpečené úložisko dát v online registračnej pokladnici (tlačiarni) posielalo údaje o predaji do tlačiarne účteniek, na zákaznícky displej a na server Finančnej správy. Len vtedy je možné zabezpečiť, že všetky údaje budú rovnaké a nemanipulovateľné. Všetky tieto zariadenia musia byť umiestnené v bezpečnom obale, ktoré zamedzí manipuláciu, či vniknutie do zariadenia vhodnou konštrukciou a predpísanou plombou.

1.5 Chránené dátové úložisko eliminuje riziko vzniku daňových únikov v režime bez online spojenia so systémom FS.

1.6 V prípade zabezpečeného dátového úložiska nie je nutné riešiť výpadky či odstavenie systému FS.

1.7 V prípade zabezpečeného dátového úložiska a automatického odosielania údajov po nadviazaní spojenia, ani maximálne doby pre odosielanie off-line účteniek, ani problémom doby odozvy systému.

1.8 Certifikácia fiškálnych zariadení zabezpečí bezpečnosť pred nekalým konaním, korektnú komunikáciu a najvyššiu pluralitu pri výbere registračného zariadenia a výbere používanej aplikácie pri najnižších nákladoch pri zachovaní vysokej bezpečnosti!

1.9 Kontrola správnosti účtovania zákazníkom - tlač účtenky na fiškálnom zariadení, z chráneného dátového úložiska, údajmi na zákazníckom displeji integrovanom v jednom zariadení pod krytom chráneným daňovou plombou.

1.10 Výtlačok účtenky a zákaznícky displej pre ochranu spotrebiteľa.

1.11 Zapečatené pokladnice a zapečatené dátové úložisko s jednoznačným identifikátorom úložiska dát - zamedzenie nezákonnej manipulácie so zariadením a s chránenými údajmi.

1.12 Jednoznačná identifikácia certifikovaného fiškálneho zariadenia a dátového úložiska.

1.13 Možnosť používania jediného fiškálneho zariadenia s konkrétnym privátnym kľúčom na mieste, kde sú vydávané účtenky.

1.14 Doriešiť Inštitút predbežnej účtenky.

1.15 Automatické odosielanie zabezpečených off-line údajov po získaní spojenia daňovou jednotkou.

1.16 Upgrade systému fiškálneho zariadenia len výrobcom, alebo importérom certifikovaným SW zariadenia.

1.17 Autorizovaní technici - servisní pracovníci pre technickú kontrolu a autorizovaný prístup do zariadenia

1.18 Požiadavky definované súčasným zákonom pre používanie ORP (online registračná pokladnica) a VRP (virtuálna registračná pokladnica) nie sú si pred zákonom rovné, hoci slúžia rovnakému účelu a vzhľadom na riziká vzniku daňových únikov pri používaní VRP, ktoré sú podstatne väčšie ako pri ORP, keďže nič z hore uvedenému VRP nespĺňa, odporúčame kompetentným prehodnotiť opodstatnenosť resp. zásadnú rekonštrukciu VRP v systéme e-kasa.

*Pripomienky k vybraným ustanoveniam zákona*

§ 2

Písm. c)

V definícii online registračnej pokladnici nie je stanovené, že chránené dátové úložisko je s registračnou pokladnicou jeden funkčný celok.

Návrh APZ: určite odporúčame, aby chránené dátové úložisko bolo s online registračnou pokladnicou a zákazníckym displejom jeden funkčný celok z dôvodu fyzickej ochrany prístupu k nosiču údajov chráneného dátového úložiska a chránené plombou.

Je nutné zabezpečiť, aby údaje v chránenom úložisku dát boli zhodné s údajmi tlačenými na účtenke, aj s údajmi zobrazovanými na displeji zákazníka. Je nutné, aby údaje neboli len zašifrované, ale aby k úložisku nebol fyzický prístup bez porušenia plomby. V súčasnosti všetky tarifikačné zariadenia ako plynomery, elektromery, vodomery a podobne majú všetky meracie, pamäťové a zobrazovacie prvky umiestnené v spoločnom bezpečnom obale zabezpečenom pred manipuláciou predpísanou plombou. Súčasné ORP túto povinnosť nemajú.

Písm. c)

Z definície online registračnej pokladnice vypadol zákaznícky displej

Návrh APZ: odporúčame zákaznícky displej zachovať, z dôvodu preventívneho nástroja na elimináciu potenciálnych daňových únikov, súvisiace zákony (zákon o ochrane spotrebiteľa, zákon o cenách) definujú povinnosti o informovanosti spotrebiteľa, zákon 208/2008 definoval ako spotrebiteľa informovať, vypustením ustanovenia vzniká právna neistota.

Správca dane uvádza, že sa počíta s posielaním účteniek mailom. V prípade vydania elektronickej účtenky, je zákaznícky displej jediná možnosť kontroly spotrebiteľa na mieste, aby mohol kontrolovať, čo mu bolo účtované.

Písm. o)

V definícii chráneného dátového úložiska nie sú stanovené požiadavky na fyzickú ochranu prístupu ku úložisku, ktoré sú nedeliteľnou súčasťou opatrení, aby sa z dátového úložiska stalo chránené dátové úložisko

Návrh APZ: Navrhujeme stanoviť požiadavky na fyzickú ochranu prístupu k nosiču údajov na chránenom dátovom úložisku. Určite odporúčame, ale aby bolo súčasťou online registračnej pokladnice alebo tlačiarne, ktoré celá by mala byť chránená tak, aby nebol možný neautorizovaný zásah do konštrukcie online registračnej pokladnice, alebo on-line tlačiarne (napr. plombou).

Písm. o)

V definícii chráneného dátového úložiska chýba požiadavka na jednoznačnú fyzickú identifikáciu každého chráneného dátového úložiska (výrobné číslo) a jeho spárovanie s podnikateľom, ktorý ho používa

Návrh APZ: odporúčame stanoviť požiadavku jednoznačnej fyzickej identifikácie chráneného dátového úložiska od výrobcu (výrobné číslo), aby bolo jednoznačne zabezpečené na ktoré chránené dátové úložisko finančné riaditeľstvo vydalo identifikátor a ktorý podnikateľ ho používa.

§ 7a

Ods. 1)

Paragraf 2 definuje identifikátor chráneného dátového úložiska, v paragrafe 7a nie sú stanovené pravidlá

pre jeho pridelenie

Návrh APZ: doplniť ku kódu pokladnice aj identifikátora (výrobné číslo) chráneného dátového úložiska, ktorý je podnikateľovi vydaný.

§ 8a

Ods. 7)

Návrh APZ: na prevádzke nesmie byť žiadna neregistrovaná online registračná pokladnica ani neregistrované chránené dátové úložisko pre potreby vydávania a ukladania daňových dokladov a dátových správ

§ 12

Návrh APZ: Zrušiť článok 5 za účelom umožnenia kontroly finančnej hotovosti na mieste pracovníkom kontroly FS.

***ELCOM (ELCOM, spoločnosť s ručením obmedzeným, Prešov)***

*Všeobecne k platnému zákonu*

Slovenska republika ma dlhoročnú tradíciu s používaním fiškálnych zariadení, ktorá siaha až do roku 1994. V súčasnosti platný zákon 289/2008 prijatý v roku 2008, bol od svojho prijatia viac ako 13x novelizovaný. To znamená, že MFSR a Finančná sprava na základe zistení z praxe, postupne upresňovala znenia zákona tak, aby sa zákon stal efektívnym nástrojom eliminácie daňových únikov.

Považujeme za nutné pokračovať v zlepšovaní toho čo sa roky vybudovalo na základe súčasných poznatkov MFSR i Finančnej správy SR i čerpať zo skúsenosti a smerovania v iných tradičných fiškálnych krajinách (Taliansko, Poľsko, Rumunsko, Maďarsko, Nemecko, Grécko, Rakúsko, Rusko, Švédsko ...). Je preukázateľne, že v týchto krajinách je jednoznačne identifikovateľný trend zvyšovania bezpečnostných štandardov ochrany fiškálnych údajov uložených vo fiškálnych zariadeniach a ich následne odosielanie na servera finančnej správy pre potreby ich následného spracovania.

Pripojenie fiškálnych zariadení online na servery FS je preto krok MFSR a FS správnym smerom. Je však nevyhnutne venovať patričnú pozornosť zvyšovaniu bezpečnostných štandardov ochrany fiškálnych údajov vo fiškálnych zariadeniach na ktorých fiškálne údaje vznikajú. Bezpečne uložené fiškálne údaje vo fiškálnych zariadeniach a ich fyzická kopia na serveroch FS je základný kameň moderných fiškálnych legislatív v tradičných fiškálnych krajinách.

V rámci pripomienkovania boli autori predloženého návrhu zákona upozorňovaní aj zo strany APZD, že súčasná verzia zákona obsahuje viacero zásadných nedostatkov, nepresností a nedorozumení, ktoré je potrebné upraviť tak, aby táto novela dokázala skutočne naplniť očakávania správcu dane v oblasti lepšieho výberu daní.

Bohužiaľ neúspešne. Súčasná prax potvrdzuje, že naše pripomienky boli a sú opodstatnené. Vybrané opatrenia, ktoré navrhujeme opätovne zapracovať do súčasného zákona, paradoxne v zákone o používaní registračných pokladníc boli pred jeho novelou v roku 2018, no novela ich zrušila bez adekvátnej náhrady. Zrušenie týchto opatrení zvyšuje v podstatnej miere riziko vzniku daňových únikov.

Problematika je pomerne rozsiahla a odborná, preto v predmetnej úprave zákona veľmi záleží na detailoch riešenia, aj paragrafového znenia. Navrhujeme overené riešenia, ktoré používajú najvyspelejšie systémy kontroly daní, prostredníctvom ktorých by sme chceli významne zvýšiť kvalitu a bezpečnosť systému na svetovú úroveň poznatkov v tejto oblasti s dodržaním zásad.

1.1 On-line je výborným bezpečnostným doplnkom existujúcich fiškálnych zariadení

1.2 Údaje ukladané v zabezpečenom elektronickom žurnále v zabezpečenom dátovom úložisku už počas vytvárania účtenky

1.3 Zabezpečené dátové úložisko musí chrániť dáta šifrovaním predpísaným spôsobom, aj zamedzením manipulácie s úložiskom plombovaním zariadenia registrovanou daňovou plombou

1.4 Je nutné doplniť, aby správne zabezpečené úložisko dát v online registračnej pokladnici (tlačiarni) posielalo údaje o predaji do tlačiarne účteniek, na zákaznícky displej a na server Finančnej správy. Len vtedy je možné zabezpečiť, že všetky údaje budú rovnaké a nemanipulovateľné. Všetky tieto zariadenia musia byť umiestnené v bezpečnom obale, ktoré zamedzí manipuláciu, či vniknutie do zariadenia vhodnou konštrukciou a predpísanou plombou.

1.5 Chránené dátové úložisko eliminuje riziko vzniku daňových únikov v režime bez online spojenia so systémom FS.

1.6 V prípade zabezpečeného dátového úložiska nie je nutné riešiť výpadky či odstavenie systému FS.

1.7 V prípade zabezpečeného dátového úložiska a automatického odosielania údajov po nadviazaní spojenia, ani maximálne doby pre odosielanie off-line účteniek, ani problémom doby odozvy systému.

1.8 Certifikácia fiškálnych zariadení zabezpečí bezpečnosť pred nekalým konaním, korektnú komunikáciu a najvyššiu pluralitu pri výbere registračného zariadenia a výbere používanej aplikácie pri najnižších nákladoch pri zachovaní vysokej bezpečnosti!

1.9 Kontrola správnosti účtovania zákazníkom - tlač účtenky na fiškálnom zariadení, z chráneného dátového úložiska, údajmi na zákazníckom displeji integrovanom v jednom zariadení pod krytom chráneným daňovou plombou.

1.10 Výtlačok účtenky a zákaznícky displej pre ochranu spotrebiteľa.

1.11 Zapečatené pokladnice a zapečatené dátové úložisko s jednoznačným identifikátorom úložiska dát - zamedzenie nezákonnej manipulácie so zariadením a s chránenými údajmi.

1.12 Jednoznačná identifikácia certifikovaného fiškálneho zariadenia a dátového úložiska.

1.13 Možnosť používania jediného fiškálneho zariadenia s konkrétnym privátnym kľúčom na mieste, kde sú vydávané účtenky.

1.14 Doriešiť Inštitút predbežnej účtenky.

1.15 Automatické odosielanie zabezpečených off-line údajov po získaní spojenia daňovou jednotkou.

1.16 Upgrade systému fiškálneho zariadenia len výrobcom, alebo importérom certifikovaným SW zariadenia.

1.17 Autorizovaní technici - servisní pracovníci pre technickú kontrolu a autorizovaný prístup do zariadenia

1.18 Požiadavky definované súčasným zákonom pre používanie ORP (online registračná pokladnica) a VRP (virtuálna registračná pokladnica) nie sú si pred zákonom rovné, hoci slúžia rovnakému účelu a vzhľadom na riziká vzniku daňových únikov pri používaní VRP, ktoré sú podstatne väčšie ako pri ORP, keďže nič z hore uvedenému VRP nespĺňa, odporúčame kompetentným prehodnotiť opodstatnenosť resp. zásadnú rekonštrukciu VRP v systéme e-kasa.

*Pripomienky k vybraným ustanoveniam zákona*

§ 2

Písm. c)

V definícii online registračnej pokladnici nie je stanovené, že chránené dátové úložisko je s registračnou pokladnicou jeden funkčný celok.

Návrh APZ: určite odporúčame, aby chránené dátové úložisko bolo s online registračnou pokladnicou a zákazníckym displejom jeden funkčný celok z dôvodu fyzickej ochrany prístupu k nosiču údajov chráneného dátového úložiska a chránené plombou.

Je nutné zabezpečiť, aby údaje v chránenom úložisku dát boli zhodné s údajmi tlačenými na účtenke, aj s údajmi zobrazovanými na displeji zákazníka. Je nutné, aby údaje neboli len zašifrované, ale aby k úložisku nebol fyzický prístup bez porušenia plomby. V súčasnosti všetky tarifikačné zariadenia ako plynomery, elektromery, vodomery a podobne majú všetky meracie, pamäťové a zobrazovacie prvky umiestnené v spoločnom bezpečnom obale zabezpečenom pred manipuláciou predpísanou plombou. Súčasné ORP túto povinnosť nemajú.

Písm. c)

Z definície online registračnej pokladnice vypadol zákaznícky displej

Návrh APZ: odporúčame zákaznícky displej zachovať, z dôvodu preventívneho nástroja na elimináciu potenciálnych daňových únikov, súvisiace zákony (zákon o ochrane spotrebiteľa, zákon o cenách) definujú povinnosti o informovanosti spotrebiteľa, zákon 208/2008 definoval ako spotrebiteľa informovať, vypustením ustanovenia vzniká právna neistota.

Správca dane uvádza, že sa počíta s posielaním účteniek mailom. V prípade vydania elektronickej účtenky, je zákaznícky displej jediná možnosť kontroly spotrebiteľa na mieste, aby mohol kontrolovať, čo mu bolo účtované.

Písm. o)

V definícii chráneného dátového úložiska nie sú stanovené požiadavky na fyzickú ochranu prístupu ku úložisku, ktoré sú nedeliteľnou súčasťou opatrení, aby sa z dátového úložiska stalo chránené dátové úložisko

Návrh APZ: Navrhujeme stanoviť požiadavky na fyzickú ochranu prístupu k nosiču údajov na chránenom dátovom úložisku. Určite odporúčame, ale aby bolo súčasťou online registračnej pokladnice alebo tlačiarne, ktoré celá by mala byť chránená tak, aby nebol možný neautorizovaný zásah do konštrukcie online registračnej pokladnice, alebo on-line tlačiarne (napr. plombou).

Písm. o)

V definícii chráneného dátového úložiska chýba požiadavka na jednoznačnú fyzickú identifikáciu každého chráneného dátového úložiska (výrobné číslo) a jeho spárovanie s podnikateľom, ktorý ho používa

Návrh APZ: odporúčame stanoviť požiadavku jednoznačnej fyzickej identifikácie chráneného dátového úložiska od výrobcu (výrobné číslo), aby bolo jednoznačne zabezpečené na ktoré chránené dátové úložisko finančné riaditeľstvo vydalo identifikátor a ktorý podnikateľ ho používa.

§ 7a

Ods. 1)

Paragraf 2 definuje identifikátor chráneného dátového úložiska, v paragrafe 7a nie sú stanovené pravidlá

pre jeho pridelenie

Návrh APZ: doplniť ku kódu pokladnice aj identifikátora (výrobné číslo) chráneného dátového úložiska, ktorý je podnikateľovi vydaný.

§ 8a

Ods. 7)

Návrh APZ: na prevádzke nesmie byť žiadna neregistrovaná online registračná pokladnica ani neregistrované chránené dátové úložisko pre potreby vydávania a ukladania daňových dokladov a dátových správ

§ 12

Návrh APZ: Zrušiť článok 5 za účelom umožnenia kontroly finančnej hotovosti na mieste pracovníkom kontroly FS.

**ASERP (Asociácia výrobcov, dovozcov a predajcov elektronických registračných pokladníc)**

Slovenská republika ma dlhoročnú tradíciu s používaním fiškálnych zariadení, ktorá siaha až do roku 1994. Považujeme za nutné pokračovať v zlepšovaní toho čo sa roky vybudovalo na základe súčasných poznatkov MFSR i Finančnej správy SR a súčasne čerpať zo skúsenosti a smerovania na jednej strane v tradičných, skúsených fiškálnych krajinách (Taliansko, Poľsko, Rumunsko, Maďarsko, Grécko, Rusko, Švédsko...) ako aj trendy na nových veľkých fiškálnych trhoch (Nemecko) . Žiadna z týchto krajín neustupuje od ukladania a ochrany fiškálnych údajov vo vyhradených fiškálnych zariadeniach podliehajúcich certifikácii, čo aj v súčasnom návrhu novely zákona je jednoznačne identifikovateľné. Je preukázateľné, že v týchto krajinách je jednoznačne identifikovateľný trend zvyšovania bezpečnostných štandardov ochrany fiškálnych údajov uložených vo fiškálnych zariadeniach ( alebo špeciálnych dátových úložiskách certifikovaných pre tento účel ) prípadne doplnený odosielaním kópii fiškálnych údajov na server finančnej správy pre potreby ich následného spracovania.

*Zhodnotenie súčasného stavu :*

Súhlasíme so stanoviskom MF SR, že súčasný cit. zákon je pre podnikateľov neprehľadný, nakoľko obsahuje okrem ustanovení týkajúcich sa používania pokladnice e-kasa klient aj ustanovenia týkajúce sa používania elektronických registračných pokladníc, ktoré sú už v súčasnej dobe obsolentné a už sa nepoužívajú. Preto je nutné zákon vyčistiť od zastaraných predpisov a pojmov a sprehľadniť.

Súčasný pokladničný zákon umožňuje podnikateľom výber medzi pokladňou pripojenou na systém eKasa a medzi VRP. Aktuálne je väčšia časť podnikateľov zapojená do systému eKasa ktorý je z pohľadu bezpečnosti a kontrolovateľnosti na vyššej úrovni a je vhodnejší a efektívnejší z pohľadu výberu daní. Preto doporučujeme ďalej rozvíjať práve tento systém a zároveň na základe už získaných skúseností vylepšiť a spresniť jeho vlastnosti a bezpečnostné prvky. Technické vybavenie používaných pokladníc eKasa klient je dobrým základom pre vytvorenie jednotného bezpečného a efektívne kontrolovateľného systému ktorý bude schopný zabezpečiť zlepšenie výberu daní a vytvorí rovnaké podmienky pre všetkých podnikateľov.

Ďalej však treba uviesť nedostatky v zabezpečení a chýbajúce bezpečnostné prvky ktoré už raz boli súčasťou zákona č. 289/2008 Z.z. a ich vynechanie znemožnilo

úspešné vykonanie hľbkových kontrol na pokladniach zamestnancami FS SR. Taktiež pre podnikateľov skomplikovalo prevádzkovanie svojich pokladní a dohľad nad nimi. Preto je nutné tieto ochranné faktory vrátiť pri novelizácii do zákona.

VRP, ktorá je aktuálne alternatívou voči systému eKasa, je podľa výsledkov štatistického úradu nerentabilným prostriedkom na výber daní. Jeho prevádzkové náklady ďaleko prevyšujú obrat peňazí ktoré boli cez túto aplikáciu vybrané do štátneho rozpočtu. Tento rozdiel sa za dané obdobie neznižoval. Technické zabezpečenie VRP nie je v súlade normami ktoré by garantovali čo len minimálne zabezpečenie proti prípadnej manipulácii s dokladmi. VRP, ako potvrdzuje aj kauza Mýtnik, je účelovým projektom, ktorý bol dlhodobo kritizovaný odbornou verejnosťou ako riešenie, ktoré znižuje kontrolné mechanizmy pri príjme hotovosti a výbere DPH. V ďalšom období bolo jeho uplatnenie a rozsah zvyšované, boli rozširované skupiny podnikateľov, ktoré mohli kontroverznú aplikáciu využívať až do dnešného stavu, kedy ju môžu využívať podnikateľské subjekty bez obmedzenia. Toto rozširovanie možno tiež chápať ako cestu k maximalizácii výnosov korupčnej skupiny vzhľadom na nemalé sumy platené za zmenové konania či správu aplikácie a infraštruktúry. Zo zmäkčovania pravidiel pre podnikateľov, ktorí môžu toto účelové riešenie používať pravdaže vyplýva aj jeho „obľúbenosť“ v podnikateľskom prostredí a „prelievanie“ povinných subjektov z prísnejšie kontrolovanej eKasy do bezplatnej nekontrolovateľnej virtuálnej pokladnice. Preto je nutné VRP ako prostriedok na výber dane zrušiť a presmerovať povinné subjekty do zabezpečeného prostredia eKasy.

Doporučujeme doplniť a zmeniť v zákone č.289/2008 :

Upraviť technický predpis pre pokladne s CHDÚ v nasledovných bodoch:

1. CHDÚ musí byť zabezpečené proti manipulácii obsahu s využitím metód elektronického podpisu, prípadne kryptovania. Obsah musí byť právne relevantný pre účely preukazovania a elektronicky exportovateľný v štandardizovanom formáte s možnosťou jednoznačne verifikovať´ pravosť obsahu.

2. Komunikácia medzi PPEKK a CHDÚ musí byť zabezpečená použitím asymetrického šifrovania, pričom verejný kľuč musí byť uložený v PPEKK a súkromný kľúč musí byť uložený v CHDÚ pre všetky riešenia

3. Všetky tlačové výstupy musia prechádzať cez CHDÚ, CHDÚ tlačové výstupy zaznamená bez zmeny 1:1.

4. Po uložení tlačových výstupov ich CHDÚ priamo odošle na pripojenú tlačiareň.

5. CHDÚ musí byť súčasťou tlačiarne s ktorou tvorí jeden funkčný celok, bez voľného prístupu užívateľa.

6. Prístup k CHDÚ bude umožnený iba poverenej osobe porušením daňovej plomby.

7. Vrátiť daňové plomby a servisné strediská.

Zdôvodnenie :

Je nevyhnutné, aby údaje nemohli byť predmetom podvodnej manipulácie, musia byť najprv uložené v správne zabezpečenom úložisku dát v online registračnej pokladnici (fiškálnej tlačiarni), Len vtedy je možné zabezpečiť, že všetky predpísané údaje budú bezpečne uložené v chránenom dátovom úložisku, budú rovnaké na účtenke aj na serveri FS SR a nemanipulovateľné. Len vtedy je možné zamedziť manipulovaniu údajov prostredníctvom dnes bežne známych spôsobov nekalého konania. Necitlivým vynechaním len niektorých bodov otvárame podvodom bránu dokorán. Tieto opatrenia boli žiaľ úplne neodborne vynechané z dnes platného zákona.

Všetky CHDU musia byť umiestnené v bezpečnom obale, ktorý zamedzí manipuláciu, či vniknutie do zariadenia vhodnou konštrukciou a predpísanou plombou. Tieto veľmi podstatné, už raz schválené ustanovenia FS SR a schválené na rozporovom konaní bez výhrad, v paragrafovom znení z neznámeho dôvodu vypadli. Absencia týchto opatrení je aj v rozpore s prijatými bezpečnostnými štandardami MF SR pre informačné systémy verejnej správy .

Všetky kontrolné zariadenia ako plynomery, elektromery, vodomery a podobne majú všetky meracie, pamäťové a zobrazovacie prvky umiestnené v spoločnom bezpečnom obale zabezpečenom pred manipuláciou predpísanou plombou. Toto zabezpečenie je všeobecne pokladané za základné a nutné bezpečnostné opatrenie a taktiež platobné karty ktoré majú v sebe citlivé údaje sú chránené šifrovaním .

Certifikácia fiškálnych zariadení zabezpečí bezpečnosť pred nekalým konaním, korektnú komunikáciu a najvyššiu pluralitu pri výbere registračného zariadenia a výbere používanej aplikácie pri najnižších nákladoch pri zachovaní vysokej bezpečnosti! Požiadavky na zariadenie a na proces certifikácie je potrebné precízne dopracovať. Chýbajú opatrenia na umiestnenie chránenej dátovej jednotky, proces ukladania údajov, povinné údaje ukladané do úložiska, ochrana údajov a komunikačných kanálov pri odosielaní do tlačiarne, zákaznícky displej a komunikačnú jednotku. Chýba predpis a kontrola opatrení týchto zariadení pred zneužitím a neautorizovanou manipuláciou – plombovanie, kontrola prepojenia, zápis do chráneného úložiska pri odpojení, manipulácii, poruche, oprave, opätovnom spustení a podobne. Tieto náležitosti vyžadujú a certifikujú všetky moderné systémy. Dávajú správcovi dane zistiť nepovolenú manipuláciu s fiškálnym zariadením. Tieto opatrenia a postupy boli precízne vypracované v predchádzajúcej legislatíve. Tieto opatrenia boli zo súčasného zákona necitlivo vypustené bez náhrady.

Zapečatené (plombované) pokladnice a zapečatené dátové úložisko s jednoznačným identifikátorom úložiska dát - zamedzenie nezákonnej manipulácie so zariadením, jeho časťami, a s chránenými údajmi a možnosti chránené dátové úložiská zamieňať. Existuje mnoho podvodov, ktoré zneužívajú nezabezpečené zariadenia, zobrazujú iné údaje na účtenke a iné údaje odosielajú na server finančnej správy.

Bez bezpečného plombovania a zabezpečenia by mohol ktokoľvek zasahovať, zamienať alebo odpájať jednotlivé časti chráneného kontrolného zariadenia. Údaje o predaji nezapisovať, alebo zapisovať do iného zariadenia, ktoré neslúži na kontrolu a záznam finančných transakcií, pozmeňovať, prípadne mazať ich.

Zákaznícke a užívatelské poznatky z praxe:

Majitelia pokladní ostali bez kontrolných záznamov ktoré im pomáhali v riadení firmy a zjednodušili účtovanie.

Na základe ich poznatkov doporučujeme :

- zaviesť povinnosť tlače dennej uzávierky

- zaviesť servisné strediská s povinnosťami ktoré pôvodný fiskálny zákon predpisoval

- zaviesť vytváranie elektronického žurnálu ktorý by sa ukladal v CHDÚ a bol by zhodný s dokladmi na serveri FS

- zaviesť povinnosť displeja ktorý by bol priamou neoddeliteľnou súčasťou pokladne a bol by primeranou kontrolou pre kupujúceho zákazníka.

V rámci liberalizácie trhu sa navrhuje zaviesť nový typ pokladnice, tzv. softvérová on-line registračná pokladnica, pričom podnikateľ sa môže rozhodnúť, či bude používať tento typ pokladnice alebo bude používať on-line registračnú pokladnicu, resp. virtuálnu registračnú pokladnicu.“

Odborná verejnosť nevidí dôvod na zavedenie ďalšieho neovereného produktu ktorý by slúžil na výber dane. Ešte sme ani neuplatnili skúsenosti z nedávno uvedeného riešenia eKasy a už je snaha opäť znižovať bezpečnostné parametre a vytvárať ďalší neoverený, hardverovými prvkami nezabezpečený systém na výber daní, ktorý by opäť priniesol iba zbytočný zmätok do existujúceho systému . Zavedenie takéhoto ďalšieho systému pokladáme za nezodpovedné. Ekasa klient s komerčnými pokladňami po zavedení sprísnených technických zabezpečení bude dostatočným prostriedkom pre výber daní a najbezpečnejším prostriedkom pre štát.

Zdôvodnenie :

Používateľ pokladnice by nebol schopný vystaviť doklad výzorovo totožný s pokladničným dokladom, ak by predajná aplikácia neumožňovala tlač takýchto podvodných dokladov. CHDÚ ukladá všetky tlačové výstupy a v prípade podozrenia sa dá jednoducho preukázať výstupná forma tlače. Ak bude CHDÚ ako ochranný a dôkazový prvok odstránený z eKASY, nebude žiaden priamy dôkaz o vystavený podvodných dokladov.

***APZD (Asociácia priemyselných zväzov a dopravy)***

*Všeobecne k platnému zákonu*

Slovenska republika ma dlhoročnú tradíciu s používaním fiškálnych zariadení, ktorá siaha až do roku 1994. V súčasnosti platný zákon č. 289/2008 Z. z. prijatý v roku 2008, bol od svojho prijatia viac ako 13x novelizovaný. To znamená, že MF SR a Finančná sprava na základe zistení z praxe, postupne upresňovala znenia zákona tak, aby sa zákon stal efektívnym nástrojom eliminácie daňových únikov.

Považujeme za nutné pokračovať v zlepšovaní toho čo sa roky vybudovalo na základe súčasných poznatkov MFSR i Finančnej správy SR i čerpať zo skúsenosti a smerovania v iných tradičných fiškálnych krajinách (Taliansko, Poľsko, Rumunsko, Maďarsko, Nemecko, Grécko, Rakúsko, Rusko, Švédsko ...). Je preukázateľne, že v týchto krajinách je jednoznačne identifikovateľný trend zvyšovania bezpečnostných štandardov ochrany fiškálnych údajov uložených vo fiškálnych zariadeniach a ich následne odosielanie na server finančnej správy pre potreby ich následného spracovania.

Pripojenie fiškálnych zariadení online na servery FS je preto krok MF SR a FS správnym smerom. Je však nevyhnutne venovať patričnú pozornosť zvyšovaniu bezpečnostných štandardov ochrany fiškálnych údajov vo fiškálnych zariadeniach, na ktorých fiškálne údaje vznikajú. Bezpečne uložené fiškálne údaje vo fiškálnych zariadeniach a ich fyzická kopia na serveroch FS je základný kameň moderných fiškálnych legislatív v tradičných fiškálnych krajinách.

V rámci pripomienkovania boli autori predloženého návrhu zákona upozorňovaní aj zo strany APZD, že súčasná verzia zákona obsahuje viacero zásadných nedostatkov, nepresností a nedorozumení, ktoré je potrebné upraviť tak, aby táto novela dokázala skutočne naplniť očakávania správcu dane v oblasti lepšieho výberu daní, avšak neúspešne. Súčasná prax potvrdzuje, že naše pripomienky boli

a sú opodstatnené. Vybrané opatrenia, ktoré navrhujeme opätovne zapracovať do súčasného zákona, paradoxne v zákone o používaní registračných pokladníc boli pred jeho novelou v roku 2018, no novela ich zrušila bez adekvátnej náhrady. Zrušenie týchto opatrení zvyšuje v podstatnej miere riziko vzniku daňových únikov.

Problematika je pomerne rozsiahla a odborná, preto v predmetnej úprave zákona veľmi záleží na detailoch riešenia, aj paragrafového znenia. Navrhujeme overené riešenia, ktoré používajú najvyspelejšie systémy kontroly daní, prostredníctvom ktorých by sme chceli významne zvýšiť kvalitu a bezpečnosť systému na svetovú úroveň poznatkov v tejto oblasti s dodržaním nasledovných zásad.

1.1 On-line je výborným bezpečnostným doplnkom existujúcich fiškálnych zariadení.

1.2 Údaje ukladané v zabezpečenom elektronickom žurnále v zabezpečenom dátovom úložisku už počas vytvárania účtenky.

1.3 Zabezpečené dátové úložisko musí chrániť dáta šifrovaním predpísaným spôsobom, aj zamedzením manipulácie s úložiskom plombovaním zariadenia registrovanou daňovou plombou.

1.4 Je nutné doplniť, aby správne zabezpečené úložisko dát v online registračnej pokladnici (tlačiarni) posielalo údaje o predaji do tlačiarne účteniek, na zákaznícky displej a na server Finančnej správy. Len vtedy je možné zabezpečiť, že všetky údaje budú rovnaké a nemanipulovateľné. Všetky tieto zariadenia musia byť umiestnené v bezpečnom obale, ktoré zamedzí manipuláciu, či vniknutie do zariadenia vhodnou konštrukciou a predpísanou plombou.

1.5 Chránené dátové úložisko eliminuje riziko vzniku daňových únikov v režime bez online spojenia so systémom FS.

1.6 V prípade zabezpečeného dátového úložiska nie je nutné riešiť výpadky či odstavenie systému FS.

1.7 V prípade zabezpečeného dátového úložiska a automatického odosielania údajov po nadviazaní spojenia, ani maximálne doby pre odosielanie off-line účteniek, ani problémom doby odozvy systému.

1.8 Certifikácia fiškálnych zariadení zabezpečí bezpečnosť pred nekalým konaním, korektnú komunikáciu a najvyššiu pluralitu pri výbere registračného zariadenia a výbere používanej aplikácie pri najnižších nákladoch pri zachovaní vysokej bezpečnosti!

1.9 Kontrola správnosti účtovania zákazníkom - tlač účtenky na fiškálnom zariadení, z chráneného dátového úložiska, údajmi na zákazníckom displeji integrovanom v jednom zariadení pod krytom chráneným daňovou plombou.

1.10 Výtlačok účtenky a zákaznícky displej pre ochranu spotrebiteľa.

1.11 Zapečatené pokladnice a zapečatené dátové úložisko s jednoznačným identifikátorom úložiska dát - zamedzenie nezákonnej manipulácie so zariadením a s chránenými údajmi.

1.12 Jednoznačná identifikácia certifikovaného fiškálneho zariadenia a dátového úložiska.

1.13 Možnosť používania jediného fiškálneho zariadenia s konkrétnym privátnym kľúčom na mieste, kde sú vydávané účtenky.

1.14 Doriešiť Inštitút predbežnej účtenky.

1.15 Automatické odosielanie zabezpečených off-line údajov po získaní spojenia daňovou jednotkou.

1.16 Upgrade systému fiškálneho zariadenia len výrobcom, alebo importérom certifikovaným SW zariadenia.

1.17 Autorizovaní technici - servisní pracovníci pre technickú kontrolu a autorizovaný prístup do zariadenia

1.18 Požiadavky definované súčasným zákonom pre používanie ORP (online registračná pokladnica) a VRP (virtuálna registračná pokladnica) nie sú si pred zákonom rovné, hoci slúžia rovnakému účelu a vzhľadom na riziká vzniku daňových únikov pri používaní VRP, ktoré sú podstatne väčšie ako pri ORP, keďže nič z hore uvedenému VRP nespĺňa, odporúčame prehodnotiť opodstatnenosť resp. zásadnú rekonštrukciu VRP v systéme e-kasa.

***APZD (Asociácia priemyselných zväzov a dopravy)***

*Podnety k vybraným ustanoveniam zákona*

K § 2 písm. c)

V definícii online registračnej pokladnici nie je stanovené, že chránené dátové úložisko je s registračnou pokladnicou jeden funkčný celok.

Odporúčame, aby chránené dátové úložisko bolo s online registračnou pokladnicou a zákazníckym displejom jeden funkčný celok z dôvodu fyzickej ochrany prístupu k nosiču údajov chráneného dátového úložiska a chránené plombou.

Je nutné zabezpečiť, aby údaje v chránenom úložisku dát boli zhodné s údajmi tlačenými na účtenke, aj s údajmi zobrazovanými na displeji zákazníka. Je nutné, aby údaje neboli len zašifrované,

ale aby k úložisku nebol fyzický prístup bez porušenia plomby. V súčasnosti všetky tarifikačné zariadenia ako plynomery, elektromery, vodomery a podobne majú všetky meracie, pamäťové a zobrazovacie prvky umiestnené v spoločnom bezpečnom obale zabezpečenom pred manipuláciou predpísanou plombou. Súčasné ORP túto povinnosť nemajú.

K § 2 písm. c)

Z definície online registračnej pokladnice vypadol zákaznícky displej. Odporúčame zákaznícky displej zachovať/doplniť v ďalšej právnej úprave, z dôvodu preventívneho nástroja na elimináciu potenciálnych daňových únikov, súvisiace zákony (zákon o ochrane spotrebiteľa, zákon o cenách) definujú povinnosti o informovanosti spotrebiteľa, zákon č. 289/2008 Z. z. definoval ako spotrebiteľa informovať, avšak vypustením tohto ustanovenia vznikla právna neistota.

Správca dane uvádza, že sa počíta s posielaním účteniek mailom. V prípade vydania elektronickej účtenky, je zákaznícky displej jediná možnosť kontroly spotrebiteľa na mieste, aby mohol kontrolovať, čo mu bolo účtované.

K § 2 písm. o)

V definícii chráneného dátového úložiska nie sú stanovené požiadavky na fyzickú ochranu prístupu k úložisku, ktoré sú nedeliteľnou súčasťou opatrení, aby sa z dátového úložiska stalo chránené dátové úložisko.

Navrhujeme stanoviť požiadavky na fyzickú ochranu prístupu k nosiču údajov na chránenom dátovom úložisku. Zároveň odporúčame, ale aby bolo súčasťou online registračnej pokladnice alebo tlačiarne, ktoré by mali byť chránené tak, aby nebol možný neautorizovaný zásah do konštrukcie online registračnej pokladnice, alebo on-line tlačiarne (napr. plombou).

K § 2.písm. o)

V definícii chráneného dátového úložiska chýba požiadavka na jednoznačnú fyzickú identifikáciu každého chráneného dátového úložiska (výrobné číslo) a jeho spárovanie s podnikateľom, ktorý ho používa.

Odporúčame stanoviť požiadavku jednoznačnej fyzickej identifikácie chráneného dátového úložiska od výrobcu (výrobné číslo), aby bolo jednoznačne zabezpečené, na ktoré chránené dátové úložisko finančné riaditeľstvo vydalo identifikátor a ktorý podnikateľ ho používa.

K § 7a ods. 1

§ 2 zákona definuje identifikátor chráneného dátového úložiska, avšak v § 7a nie sú stanovené pravidlá

pre jeho pridelenie. Navrhujeme doplniť ku kódu pokladnice aj identifikátor (výrobné číslo) chráneného dátového úložiska, ktorý je podnikateľovi vydaný.

K § 8a ods. 7

Navrhujeme v § 8a doplniť v odseku 7 ustanovenie tak, že na prevádzke nesmie byť žiadna neregistrovaná online registračná pokladnica ani neregistrované chránené dátové úložisko pre potreby vydávania a ukladania daňových dokladov a dátových správ.

K § 12

Navrhujeme v § 12 vypustiť odsek 5 za účelom umožnenia kontroly finančnej hotovosti na mieste pracovníkom kontroly FS.

***SAPPO (Slovenská asociácia petrolejárskeho priemyslu a obchodu)***

Za Slovenskú asociáciu petrolejárskeho priemyslu a obchodu vítame legislatívnu iniciatívu zameranú na sprehľadnenie existujúcej legislatívy, ktorej predmetom je úprava registračných pokladníc. Avšak z publikovanej predbežnej informácie (PI/2021/233) ďalej ako „PI“ nie je zrejmé, či zámerom je len sprehľadnenie právneho predpisu vypustením nerelevantných ustanovení, alebo aj systémové zmeny, v systéme nastavení on-line pokladníc, nakoľko v publikovanej PI sa uvádza, že predmetom budú aj zmeny vo vzťahu k novým trendom v evidencii tržieb. Z uvedeného však nie je možné poznať aké zmeny je možné očakávať. Zároveň, PI ďalej uvádza, že sa zavedie aj nový typ pokladnice bez bližšej charakteristiky, či definovania jej aplikability tak, aby podnikatelia vedeli predpokladať prípadnú administratívnu alebo nákladovú náročnosť.

Popri uvedenom zároveň navrhujeme aby predkladateľ tiež zvážil prehodnotiť súčasnú právnu úpravu s ohľadom k tzv. CHDU, pamäťovým modulom ako aj subsekventným povinnostiam podnikateľov z pohľadu ich archivácie či evidencie, nakoľko PI uvádza aplikáciu najnovších trendov a elimináciu obsolentných technológii.

Taktiež v rámci zosúladenia s reálnou situáciou na Slovensku, odporúčame v návrhu právneho predpisu zvážiť úpravu predĺženia 48 hodinovej lehoty na obnovenie prevádzky pokladnice alebo zariadenia od vzniku poruchy pokiaľ príde k výpadku online pripojenia, keďže zákon nepočíta so skutočnosťou, že niektoré prevádzky sú ťažko dostupné alebo majú časté výpadky internetového pripojenie (napr. v prípade niektorých diaľničných čerpacích staníc, kde sú žiaľ takéto výpadky veľmi bežné).