Příloha n)

Organizačního řádu

OCHRANA A ZPRACOVÁNÍ CITLIVÝCH INFORMACÍ

Článek I.

Kodex zaměstnance ve styku s citlivými informacemi

Ochrana osobních údajů, ochrana soukromí a práv každého jednotlivce je jednou ze základních hodnot, které zaměstnanci společnosti komory dodržují.

Zaměstnanec si plně uvědomuje hodnotu a citlivost osobních údajů, se kterými přichází do styku a se kterými pracuje. Je si plně vědom škod, které může vyzrazení, zničení nebo nežádoucí pozměnění těchto údajů způsobit každému jednomu majiteli těchto údajů.

Každý zaměstnanec se osobně zavazuje chránit důvěrnost, dostupnost a neporušenost osobních údajů, se kterými přichází do styku a se kterými pracuje, protože to považuje za věc své osobní profesní cti bez ohledu na to, jestli jej k tomu zavazuje právní akt.

Osobní údaje, se kterými přichází do styku a se kterými pracuje, nikdy nezveřejní, nikomu nepředá, nikdy je nepozmění nebo nezničí, mimo rozsah stanovený náplní práce.

Osobní údaje, se kterými přichází do styku a se kterými pracuje, považuje za důvěrné i ve svém soukromém životě. A bude je chránit i po ukončení pracovního poměru.

Aby se zaměstnanec vyhnul nezamýšlenému vyzrazení, zničení nebo nežádoucímu pozměnění osobních údajů, se kterými přichází do styku a se kterými pracuje, pravidelně se v dané oblasti vzdělává.

Každý zaměstnanec věnuje maximální úsilí tomu, aby zabránil vyzrazení, zničení nebo nežádoucímu pozměnění osobních údajů, se kterými přichází do styku a se kterými pracuje. To znamená, že dodržuje bezpečnostní opatření informační bezpečnosti (obecná pravidla fyzické i kybernetické bezpečnosti citlivých informací a bezpečnostní desatero), chrání osobní údaje v listinné podobě (udržuje na pracovišti pořádek, uzamyká kancelář, ukládá listiny na určená místa = nenechává je na pracovním stole), všímá si svého okolí a neprodleně hlásí jakékoliv podezřelé chování výpočetní techniky, svých kolegů nebo třetích stran (návštěv areálu komory).

Komora a její každý člen i zaměstnanec věnuje maximální úsilí tomu, aby bylo zajištěno spravedlivé a transparentní zpracování osobních údajů, za tímto účelem, jsou zpracovány procesy, které nepřetržitě vylepšujeme tak, aby každý subjekt měl v každém okamžiku k dispozici odpověď na jakoukoliv otázku týkající se jeho osobních údajů a jejich zpracování.

Komora a její každý člen i zaměstnanec věnuje maximální úsilí tomu, aby bylo zajištěno naplnění práv subjektů osobních údajů, a za tímto účelem jsou implementovány jednak odpovídající technologie a jednak zavedeny správné procesy.

Osoby pracující s citlivými (osobními) údaji nevytváří zbytečné elektronické nebo tištěné kopie dokumentů tyto údaje obsahující. Při likvidaci dokumentů s těmito údaji dle požadavků Archivačního a skartačního řádu na jejich životní cyklus je zapotřebí posoudit i nutnost řešit tytéž požadavky na veškeré pořízené kopie. Odpovědnost za dodržování těchto požadavků má každý zaměstnanec za svou agendu.

Článek II.

Bezpečnostní desatero ochrany citlivých informací

Komora dbá na bezpečnost osobních údajů, dat a informací. Všechna bezpečnostní opatření a bezpečnostní mechanismy jsou však neúčinné pokud není dodržován elementární bezpečnostní přístup uživatelů informačního systému.

V této souvislosti je níže uvedeno několik základních pravidel, které je potřeba mít neustále na paměti.

1. Při jakkoli krátkém opuštění svého pracovního místa je nutné zamknout pracovní stanici;
2. Při jakkoli krátkém opuštění svého pracovního místa je třeba veškeré materiály, které svým charakterem obsahuji citlivé informace (osobní údaje, interní informace, apod.) alespoň uložit do zásuvky – tzv. zásada čistého pracovního stolu; obzvláště to platí pro ty, kteří přicházejí v kanceláři ke styku s třetími stranami (zákazníci, dodavatelé atp.);
3. Při pořizování kopií a skenování je potřeba se přesvědčit, zda v kopírce/skeneru nezůstal originál dokumentu. Při likvidaci dokumentů s osobními údaji, kterým vypršela lhůta životnosti, je nutné zlikvidovat také všechny kopie takovýchto dokumentů;
4. Při tisku dokumentů, které svým charakter odpovídají citlivé informaci, je potřeba si tisk okamžitě vyzvednout u tiskárny, a to v případě tisku na sdílené stroje. Je potřeba mít přitom na zřeteli i dokumenty, které se „zaseknou" v tiskové frontě a mohly by se vytisknout „samy" později. Stejně tak je potřeba se přesvědčit, zda netisknete náhodou na jinou než zamýšlenou tiskárnu;
5. V případě elektronické komunikace, zkontrolujte adresáta emailu, aby zpráva nebyla omylem odeslána nezamýšlené osobě. Nepřeposílejte obsah komunikace s třetí osobou a pokud to není nutné, nepoužívejte volbu „odpovědět všem" – Reply to all.
6. Citlivé informace je povoleno ukládat jen na zabezpečená interní datová uložiště. Je zakázáno ukládat citlivá a nezabezpečená data (šifrováním nebo dostatečně silným heslem) na cloudová uložiště (DropBox, SkyDrive apod.). Je zakázáno zaměstnancům komory ukládat citlivá data na přenosná úložiště (např. přenosné USB disky) bez vědomí a předchozího souhlasu ředitele;
7. Při práci s elektronickou poštou je potřeba být obezřetný a dostatečně rezistentní vůči emailům s podvodným a potencionálně nebezpečným obsahem. Neotevírat a neklikat v emailu na odkazy a neotevírat přílohy, pokud není jistota pravosti obsahu – věrohodný odesilatel, informace v emailu a případně adresy uvedených odkazů. Nezapomeňte na to, že email je snadné zfalšovat a podvrhnout;
8. Na prostředcích komory a na všech prostředcích, které jsou připojeny do sítě komory, není dovoleno navštěvovat internetové stránky s potenciálně nebezpečným obsahem (erotické stránky, „warez" stránky apod.) a taktéž z internetu stahovat obsah, který nesouvisí s pracovní činností (jakýkoliv software a datové soubory). Svěřené pracovní prostředky nejsou určeny k soukromým účelům. Není povoleno připojovat zaměstnancům neautorizovaná USB zařízení;
9. Je potřeba kontrolovat a zavírat za sebou vstupní dveře, které oddělují veřejně dostupné prostory od interních a být obezřetný ke komukoli, koho neznáte. Ti, kteří mají přístup do serverovny a jiných neveřejných prostor, se před odchodem musí přesvědčit, že za sebou nenechali otevřené a nezamčené dveře;
10. Při zjištění nějakého rizika souvisejícího s informační bezpečnosti, podezřelé činnosti osob, nezvyklého chování informačních systémů či přímo bezpečnostního incidentu, je toto třeba neprodleně nahlásit na e-mail koberna@foodnet.cz nebo řediteli pro programování a strategii osobně, aby bylo možné včas situaci řešit a případně přijmout nápravná opatření.

Tato Příloha o ochraně a zpracování citlivých informací nabývá platnosti a účinnosti dnem 1. 11. 2018.

Příloha o)

Organizačního řádu

ŘÍZENÍ BEZPEČNOSTNÍCH INCIDENTŮ K OCHRANĚ OSOBNÍCH ÚDAJŮ

Článek I.

Úvodní ustanovení

Účel dokumentu:

Účelem této směrnice pro Řízení bezpečnostních incidentů k ochraně osobních údajů (dále jen „směrnice") je řízení činností, procesů, kompetencí a odpovědností souvisejících se zaznamenáním, vyhodnocením, řešením a předcházením fyzickým a IT bezpečnostních incidentů v komoře.

Závaznost dokumentu:

1. Tato směrnice je závazná pro řízení činností, procesů, kompetencí a odpovědností souvisejících se zaznamenáním, vyhodnocením, řešením a předcházením IT bezpečnostních incidentů v komoře.

2. Požadavky této směrnice jsou závazné i pro všechny externí subjekty, které mají přístup k informačním systémům a datům komory (outsourceři, dodavatelé, konzultanti, atd.).

Zodpovědnost v oblasti řízení incidentů:

1. Hlásit bezpečnostní událost, potažmo bezpečnostní incident jsou povinni všichni zaměstnanci komory a uživatelé IS komory a dále pak i všechny externí subjekty, které mají přístup k informačním systémům a datům komory (outsourceři, dodavatelé, konzultanti, atd.).

2. Za návrh řešení, analýzu a návrh vypořádání bezpečnostního incidentu zodpovídá ředitel pro programování a strategii. Tím je předkládána zpráva o bezpečnostním incidentu vedení komory, které je odpovědné za schválení nápravných opatření navržených ředitelem pro programování a strategii vyplývající z analýzy bezpečnostního incidentu.

3. Ředitel pro programování a strategii vede evidenci o bezpečnostních incidentech a zodpovídá za dodržení celého procesu odstranění následků incidentu, případně hlášení Úřadu pro ochranu osobních údajů a dotčeným subjektům údajů.

Článek II.

Bezpečnostní incident

Kategorie bezpečnostního incidentu:

1. Komora pracuje s incidenty podle jejich příčiny:

   a. narušení schválených interních pravidel v oblasti fyzické bezpečnosti OU,
   b. narušení schválených interních pravidel v oblasti bezpečnosti IT a elektronické podoby OU
   c. narušení bezpečnosti z vnějšího prostředí (obvykle útočníkem nebo útočníky)

2. Komora pracuje s incidenty také podle jejich závažnosti:

a. Běžný bezpečnostní incident – došlo k porušení nebo neúspěšnému pokusu o porušení důvěrnosti, integrity a dostupnosti v rozsahu, který neodpovídá Závažnému bezpečnostnímu incidentu. Příklad: událostí je zachycení škodlivého kódu antivirovým systémem.
b. Závažný bezpečnostní incident – došlo k úspěšnému porušení důvěrnosti, integrity a dostupnosti v rozsahu, kdy jsou dotčeny osobní údaje členů nebo zaměstnanců komory. Takový incident je nutno do 72 hodin od jeho zjištění nahlásit včetně popisu přijatých opatření a záznamů o činnostech zpracování Úřadu pro ochranu osobních údajů a představuje-li incident významné riziko pro zneužití identity, je nutné jej také oznámit dotčeným subjektům údajů. Příklad: incidentem je, pokud dojde k zavirování počítače, nežádoucímu zašifrování dat

Postup řešení bezpečnostního incidentu:

1. Pokud uživatel (nebo pracovník externího subjektu), který má přístup k informačním systémům a datům komory (outsourceři, dodavatelé, konzultanti, atd.) zpozoruje nebo odhalí jakoukoliv podezřelou nebo neobvyklou činnost, která je v rozporu s bezpečnostní politikou nebo je nestandardní (jedná se jak o chování IS, tak o chování osob či změny prostředí) je povinen tuto neprodleně ohlásit svému nadřízenému, nebo řediteli komory.

2. Uživatel ohlásí bezpečnostní incident řediteli pro programování a strategii prostřednictvím emailu, telefonicky nebo zprostředkovaně jinou osobou/uživatelem a to tak, aby bylo zamezeno jakýmkoliv zbytečným prodlením.

3. Hodnocení incidentu, návrh a realizace okamžitého řešení pro zamezení škod je prováděno neprodleně ředitelem pro programování a strategii.

4. Ředitel pro programování a strategii provede

   a. vyhodnocení incidentu
   b. určí řešení
   c. rozhodne, zda je nutné neprodleně informovat UOOU, případně dotčené SU
   d. informuje prezidenta Komory
   e. provede formální uzavření (vznikne záznam).

5. Pracovníci IT (nebo odpovědnou osobu v případě ne IT událostí) provedou vyhodnocení události a určí, zdali se jedná o bezpečnostní událost nebo incident. Určí a provedou okamžitě opatření, které zamezí dalším škodám. Vedoucí IT (nebo odpovědnou osobu v případě ne IT událostí) určí odpovídajícího řešitele, který zajistí provedení opatření. Ten po jejich dokončení informuje vedoucího IT (nebo odpovědnou osobu za oddělení ne-IT událostí), který následně podá informace bezpečnostnímu manažerovi komory, který provede formální uzavření (vznikne záznam).

6. Veškeré záznamy o bezpečnostním incidentu jsou po jeho ukončení předány bezpečnostním /manažerem IT, vedoucímu odpovídajícího oddělení k analýze. Cílem analýzy je identifikovat kořenové příčiny a zamezit opakování incidentu.

7. Analýza incidentu, návrh a realizace nápravného opatření je prováděno pracovníky IT nebo odpovědnou osobu. Je neprodleně zpracována zpráva, která obsahuje:

   a. Časové údaje – kdy došlo k události/incidentu
   b. Jednotlivé činitele – kdo, co
   c. Popis události – jak probíhal incident/událost
   d. Příčiny události – proč k události došlo, např. nový virus AV nezná, uživatel stáhnul atd.
   e. Kudy došlo k průniku do sítě např. USB, download, email.
   f. Je ještě uvnitř útočník? Kód, útočník, backdoor?
   g. Návrh na nápravná opatření s termínem uskutečnění nápravných opatření.

8. Odpovědná osoba komory provede hodnocení incidentu, hodnocení postupu a návrhu řešení. Může navrhnout změnu řešení, alternativní řešení, požadovat jiné řešení atd. Je možné vyvolat jednání k návrhu řešení a prodiskutovat proč není návrh akceptovatelný atd. Pokud nebudou do 7 dní vzneseny připomínky, má se za to, že návrhy jsou bez připomínek. IT vypracuje návrh řešení, který bude uvažovat všechny vznesené připomínky. Návrh řešení v reakci na připomínky bude zpracována do 14 dní od vznesení připomínek.

9. Odpovědná osoba formálně předá návrh nápravných opatření k naplánování jejich realizace.

10. Odpovědná osoba vypracuje zprávu pro prezidenta komory.

Hlášení bezpečnostních událostí a incidentů:

Odpovědná role	Personální obsazení	Kontakty	
		telefon:	e-mail:
IT	Ing. Tomáš Vacek	783 580 491	vacek@foodservis.cz
Bezpečnost	Bc. Kristina Tomanová	702 062 962	tomanova@foodnet.cz
Konzultant ochrany osobních údajů	Ing. Miroslav Koberna, CSc.	603 582 215	koberna@foodnet.cz

1. V hlášení je třeba uvést informace v minimálním rozsahu:

   a. datum a čas zjištění incidentu (závady, poruchy, slabiny apod.),
   b. počítač, systém, aplikace, prostředek, příp. postižené místo (lokalita, kancelář),
   c. způsob, jakým se incident projevuje,
   d. rozsah působení incidentu (částečná funkčnost, nefunkčnost, zpomalení, nedostupnost apod.).

Činnost konzultanta ochrany osobních údajů v případě bezpečnostního incidentu týkajícího se osobních údajů:

1. Konzultant ochrany osobních údajů (dále jen KOOU) je informován bezpečnostním manažerem o bezpečnostním incidentu s možným dopadem na osobní údaje.

2. KOOU provede vyhodnocení situace, analýzu rizik osobním údajům a zpracuje návrh opatření.

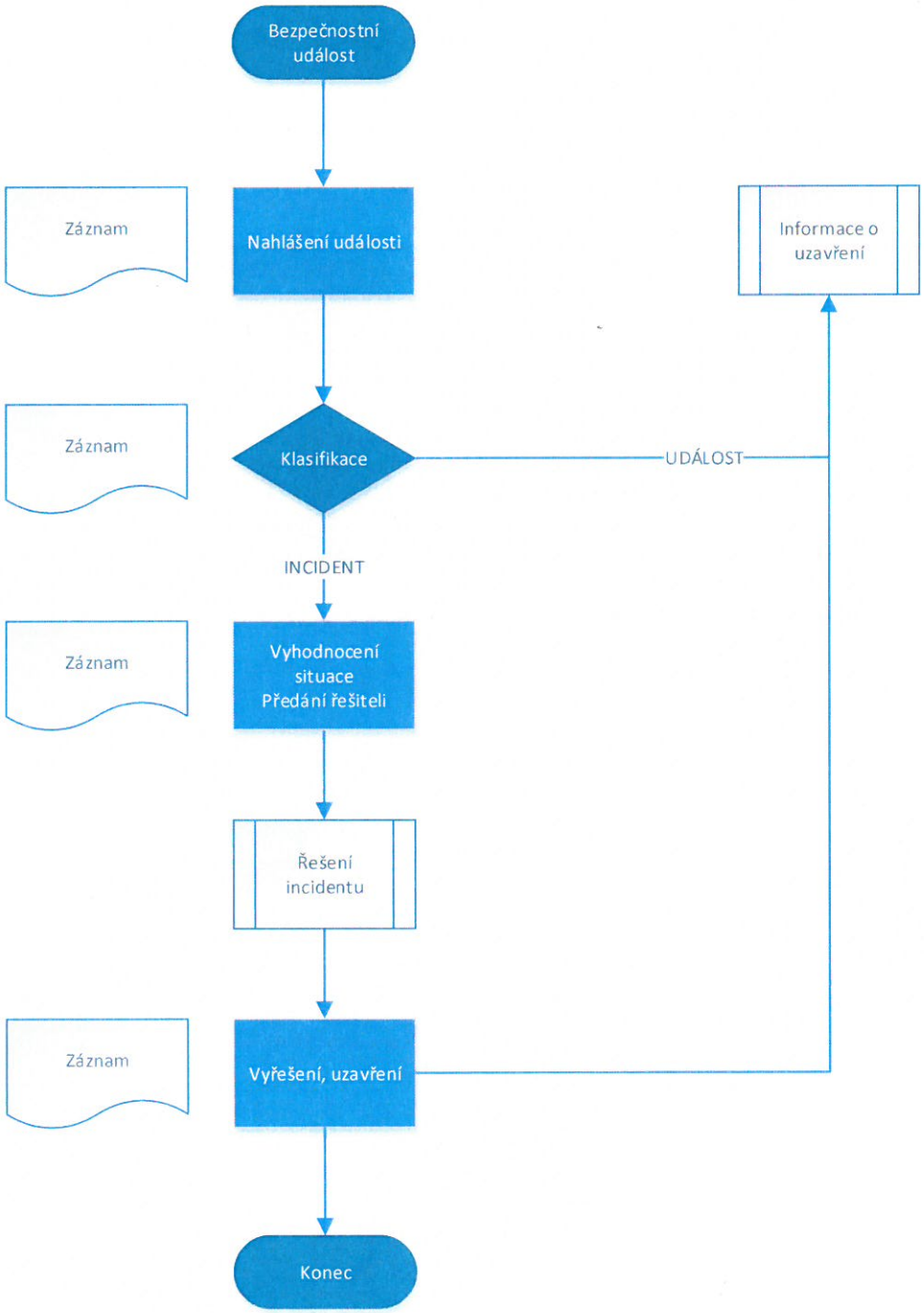
3. KOOU informuje o bezpečnostním incidentu a o navržených bezpečnostních opatřeních Úřad na ochranu osobních údajů. Informace o incidentu je provedena do 72 hodin od zjištění incidentu, i kdyby v daném okamžiku ještě neexistoval návrh nápravných opatření.

4. Pokud jsou splněny podmínky uvedené v GDPR – dojde k incidentu se závažným dopadem na subjekty osobních údajů, zajistí KOOU jejich informování o této skutečnosti, je-li to možné (přímé, nepřímé oslovení).

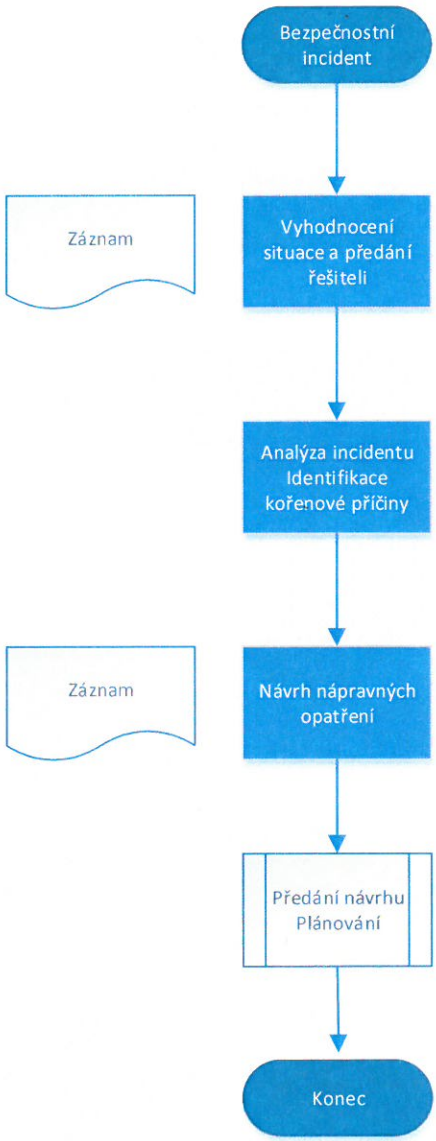
Článek III.

Diagramy řešení bezpečnostního incidentu

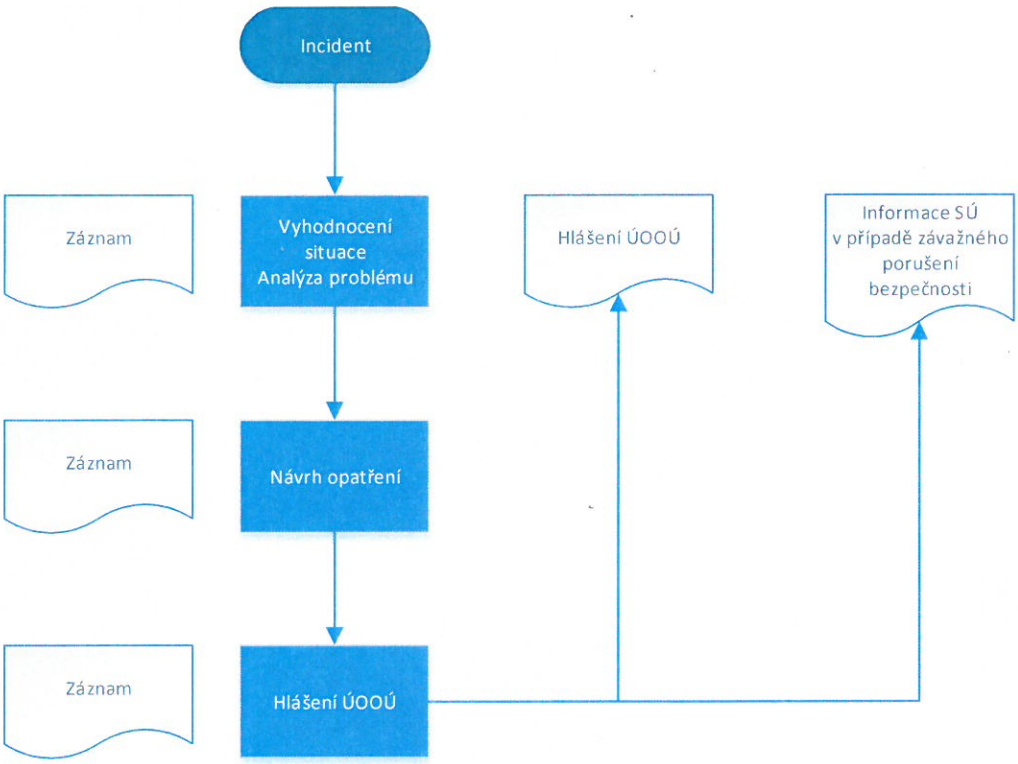
Řešení bezpečnostního incidentu:



Analýza bezpečnostního incidentu:



Činnost KOOU:



Článek IV.

Závěrečná ustanovení

Bezpečnost spravovaných informací je zodpovědností každého zaměstnance, kterému byly tyto informace svěřeny, který je ke své práci využívá i který se k informacím dostal náhodně. Nedodržení obecných pravidel bezpečnosti a výše uvedených požadavků bude posuzováno jako porušení pracovních povinností.

Tato Příloha o řízení bezpečnostních incidentů k ochraně osobních údajů nabývá platnosti a účinnosti dnem 1. 11. 2018.