\ 17.10.2024
\ Plzeň

Bezpečnost dodavatelských řetězců a smlouvy s dodavateli v praxi

\ JUDr. Mgr. Barbora Vlachová, Ph.D., LL.M.

PORTOS
Strategic Legal Advisory

Strategic Legal Advisory PORTOS

Současná právní úprava

- **Směrnice NIS** – 2016/1148, z 6. 7. 2016, o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii
- **Zákon ZKB** - 181/2014 Sb. o kybernetické bezpečnosti
- **Vyhláška VKB** – vyhláška č. 82/2018 Sb. o kybernetické bezpečnosti
- Oblast řízení dodavatelů zejm.:
  - příloha č. 7 VKB
  - § 4 odst. 4 ZKB

Strategic Legal Advisory PORTOS

Nová právní úprava

- **Směrnice NIS 2**
- Implementační lhůta – **do 17. října 2024 (dnes)**
  - Nyní je zřejmé, že tato **lhůta nebyla dodržena**
- **Zákon kybernetické bezpečnosti** + prováděcí předpisy
  - Legislativní rada vlády doporučila vládě schválení
  - Aktuálně v Poslanecké sněmovně
- Součástí nového zákona je i **mechanismus prověřování bezpečnosti dodavatelského řetězce**, který byl původně plánován jako samostatný zákon

X mimo rámec Směrnice NIS 2

Strategic Legal Advisory PORTOS

Řízení dodavatelů dle současné právní úpravy

- Dle § 8 VKB musí povinná osoba **řídit rizika spojená s dodavateli**
- Při výběru dodavatele nutné zohlednit stanovená bezpečnostní opatření dle výsledku analýzy rizik
- U významných dodavatelů je nezbytné **zohlednit oblasti uvedené v příloze č. 7 VKB + vést evidenci významných dodavatelů**
- Veškerá rizika spojená s dodavateli posuzují samotné povinné osoby
- Povinné osoby musí varování či doporučení NÚKIB zohlednit v analýze rizik a následně výsledky promítnout do zadávacích podmínek
- Aplikace § 4 odst. 4 ZKB
  - Zohlednění požadavků vyplývajících z bezpečnostních opatření v míře nezbytné pro splnění povinností podle ZKB nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži

Strategic Legal Advisory PORTOS

Požadavky na smlouvy s významnými dodavateli

- **Příloha č. 7 VKB (vybrané oblasti)**
  - Ustanovení o bezpečnosti informací (z pohledu důvěrnosti, dostupnosti a integrity)
  - Ustanovení o oprávnění užívat data,
  - Ustanovení upravující řetězení dodavatelů, přičemž musí být zajištěno, že poddodavatelé se zaváží dodržovat v plném rozsahu ujednání mezi povinnou osobou a dodavatelem
  - Ustanovení o řízení změn,
  - Specifikace podmínek pro řízení kontinuity činností v souvislosti s dodavateli (například zahrnutí dodavatelů do havarijních plánů, úkoly dodavatelů při aktivaci řízení kontinuity činností)
  - Ustanovení o právu odstoupit od smlouvy v případě významné změny kontroly nad dodavatelem nebo změny kontroly nad zásadními aktivy využívanými dodavatelem
  - Ustanovení o sankcích za porušení povinností
  - …..

Strategic Legal Advisory PORTOS

Požadavky na smlouvy s významnými dodavateli II

- Vysvětlení požadavků na smlouvy s významnými dodavateli obsahuje podpůrný materiál NÚKIB *„Požadavky na smlouvy s dodavateli“*
  - Dostupný zde: https://www.nukib.cz/download/publikace/podpurne_materialy/pozadavky_na_smlouvy_s_dodavateli_v1.4.pdf
- **Plnění povinností dle přílohy č. 7 VKB v praxi**
  - Nutné určit ve smlouvě, že je dodavatel významným dodavatelem, popř. takového dodavatele o této skutečnosti prokazatelně písemně informovat o tom vč. uvedení jeho konkrétních povinností
  - Požadavky lze zahrnout do obchodních podmínek nebo smluvních vzorů
  - Nutné určovat jednotlivé požadavky individuálně, nelze odkázat na „plnění všech povinností dle ZKB“
  - Není vhodné jít cestou „maximální přísnosti“

Strategic Legal Advisory PORTOS

Regulace smluv s dodavateli dle NIS 2

- **Čl. 85 recitálu NIS 2**: Základní a důležité subjekty by měly být zejména vybízeny, aby začlenily opatření k řízení kybernetických bezpečnostních rizik do smluvních ujednání se svými přímými dodavateli a poskytovateli služeb.
- **Čl. 21 NIS 2**: základní a důležité subjekty by měly přijmout přiměřená technická, provozní a organizační opatření k řízení bezpečnostních rizik, které zahrnují i:
- *bezpečnost dodavatelského řetězce včetně bezpečnostních aspektů týkajících se vztahů mezi každým subjektem a jeho přímými dodavateli nebo poskytovateli služeb;*
- **Čl. 22 NIS 2**: Koordinované posouzení bezpečnostních rizik kritických dodavatelských řetězců na unijní úrovni (Komise + ENISA)

Strategic Legal Advisory PORTOS

Řízení dodavatelů v návrhu zákona o kybernetické bezpečnosti

- Návrh vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností plně přebírá dosavadní principy řízení dodavatelů dle ZKB a VKB
- Návrh zákona ruší dosavadní kategorii „provozovatelů“, ponechává však kategorii významných dodavatelů
- Nově je zaveden tzv. **mechanismus prověřování bezpečnosti dodavatelského řetězce**

Strategic Legal Advisory PORTOS

Mechanismus prověřování dodavatelského řetězce

- Součástí návrhu nové legislativy v oblasti kybernetické bezpečnosti je **mechanismus prověřování bezpečnosti dodavatelského řetězce**
  - Bezpečnostní rada státu pověřila v červnu 2022 NÚKIB přípravou zákona, který bude umožňovat prověření dodavatelů do strategicky významné infrastruktury
  - Bylo rozhodnuto, že mechanismus prověřování bezpečnosti dodavatelského řetězce ale bude spojen s implementací Směrnice NIS2
- Hlavní cíl mechanismu - **možnost vyloučit z dodávek do strategicky významné infrastruktury vysoce rizikové dodavatele**
- NÚKIB bude za účelem prověřování rizik spojených s **dodavatelem poskytovatele strategicky významné služby** shromažďovat a vyhodnocovat informace a data o tom, kdo přímo nebo zprostředkovaně poskytuje plnění do strategicky významné služby
- NÚKIB **opatřením obecné povahy** stanoví podmínky poskytovatelům strategicky významných služeb, nebo zakáže využití plnění dodavatele bezpečnostně významné dodávky v kritické části stanoveného rozsahu, zjistí-li na základě vyhodnocení rizikovosti dodavatele významné ohrožení bezpečnosti České republiky nebo vnitřního pořádku

Strategic Legal Advisory PORTOS

Mechanismus prověřování dodavatelského řetězce – dopady na povinné osoby

- Povinná osoba = **poskytovatel strategicky významné služby**
- Ani u poskytovatelů strategicky významných služeb se mechanismus prověřování nevztahuje na veškeré dodávky, resp. celou jejich infrastrukturu, ale pouze na tzv. **bezpečnostně významné dodávky**, které:
  - *směřují do části systému, kterou si sami poskytovatelé určí jako kritickou – tzv. kritická část stanoveného rozsahu (aktiva s kritickým nebo vysokým dopadem na službu), a případně*
  - *souvisí se zajišťováním služby, kterou NÚKIB ve vyhlášce určí jako nepominutelnou, což se týká strategicky významných služeb pouze v některých odvětvích*
- Konkrétní rozsah působnosti mechanismu tak významně ovlivňuje i sám poskytovatel strategicky významné služby

Mechanismus prověřování dodavatelského řetězce – dopady na povinné osoby II

- Nově povinnost zjišťovat a dokumentovat informace o dodavatelích (i poddodavatelích!) bezpečnostně významných dodávek - tyto hlásit NÚKIB, včetně změn
- Zvýšená nejistota v této oblasti – k zákazu může dojít kdykoliv v době trvání závazku
- Vhodná úprava smluvních vztahů s dodavateli kvůli možnosti vydání OOP
- Veřejný zadavatel může závazek ze smlouvy na veřejnou zakázku vypovědět bez zbytečného odkladu poté, co zjistí, že v jejím plnění nelze pokračovat, aniž by bylo porušeno OOP
- Sledování procesu přijímání OOP, připomínkování návrhu OOP, tvorba žádostí o udělení výjimky

PORTOS

Strategic
Legal Advisory

Kontakt

JUDr. Barbora Vlachová, Ph.D., LL.M.

vlachova@portos.cz

T \ 00 420 224 827 884
W \ portos.cz

Hvězdova 1716/2b
140 00 Prague 4
Czech Republic