

**ZMLUVY
PRE
KYBERNETICKÚ BEZPEČNOST'**

JUDr. Štefan Pilár



BUKOVINSKÝ & CHLIPALA

ADVOKATSKA KANCELARIA • LAW FIRM • RECHTSANWALTE

Bukovinsky & Chlipala, s.r.o.

Svatoplukova 30, 821 08 Bratislava

tel. +421.2.3301.4760, +421.948.553.160

www.bch.sk, spilar@bch.sk

Member of



Partner



2019 | 2018 | 2017 | 2016 | 2015 | 2014

Slovak Leading Law Firm

Telecommunication & IT Law | Intellectual Property

Highly Recommended Law Firm

ZMLUVNÉ VZŤAHY

podľa zákona č. 69/2018 Z.z.

o kybernetickej bezpečnosti ("ZoKB")

OBSAH

- zmluva podľa § 19/2 a § 22/4 ZoKB
- komparácia s GDPR
- zmluvné dojednania podľa ZoITVS

I. 2x Zmluva o plnení bezpečnostných opatrení
a notifikačných povinností

II. „Zmluva“

III. Zmluva o využívaní akreditovanej jednotky
CSIRT

IV. Zmluva o spôsobe a forme hlásenia
kybernetických bezpečnostných incidentov

PZS a PDS

V. 2x Dohoda

I.1

§ 19 ods. 2 ZoKB

§ 8 Vyhlášky NBÚ č. 362/2018 Z.z. ("V")

Zmluva medzi prevádzkovateľom základnej služby a tretou stranou

Tretia strana

dodávateľ na výkon činností, ktoré priamo súvisia s prevádzkou sietí a informačných systémov pre prevádzkovateľa základnej služby

môže byť aj PDS?

(A) Bezpečnostné opatrenia

- technické zraniteľnosti systémov a zariadení § 9 V
- riadenie bezpečnosti sietí a informačných systémov § 10 V
- riadenie prístupov § 12 V
- riešenie kybernetických bezpečnostných incidentov § 14 V
- monitorovanie, testovanie bezpečnosti a bezpečnostných auditov § 15 V

na základe analýzy rizík
podľa § 8 ods. 1 Vyhlášky

*riziká dodávateľských služieb, akvizície, vývoja a
údržby informačných systémov spôsobom podľa § 6
Vyhlášky*

o.i. URČENIE VLASTNÍKA RIZIKA!!!

(B) Notifikačné povinnosti

- informovanie PZS o KBI a o všetkých skutočnostiach majúcich vplyv na zabezpečovanie KB § 8 ods. 2 písm. j) V
- hlásenie ďalších informácií požadovaných PZS na plnenie jeho povinností vyplývajúcich zo ZoKB a ich vymedzenie § 8 ods. 2 písm. k) V
- hlásenie všetkých informácií majúcich vplyv na ZoKB § 8 ods. 2 písm. l) V

(C) Ďalšie povinnosti

napr.:

záväzok tretej strany po ukončení zmluvy udelit', poskytnúť, previesť alebo postúpiť všetky potrebné licencie, práva alebo súhlasy nevyhnutné na zabezpečenie kontinuity prevádzkovananej základnej služby na PZS, a to po dobu aspoň päť rokov po ukončení zmluvného vzťahu

LEHOTA

do dvoch rokov od účinnosti ZoKB

01.04.2018 – 01.04.2020

I.2

Zmluva o plnení bezpečnostných opatrení a notifikačných povinností

§ 22 ods. 4 ZoKB

Zmluva medzi poskytovateľom digitálnej služby a prevádzkovateľom základnej služby

(...nie tret'ou stranou / subdodávateľom???)

Dôvodová správa

k § 22 ZoKB

odsek 4 a 5 upravuje nevyhnutné povinnosti

PDS vo vzťahu k tretím stranám

Náležitosti?

...inšpirácia Vyhláškou...

II.

”Zmluva”

§ 22 ods. 5 ZoKB

*povinnosť poskytovateľa digitálnej služby o
hlásenom kybernetickom bezpečnostnom
incidente v nevyhnutnom rozsahu informovať
tretiu stranu, ak by sa plnenie zmluvy stalo
nemožným*

aká zmluva (§ 19 ods. 4 ZoKB)???

kto je tretia strana???

...subdodávateľ

*„ustanovenie o povinnosti dodržiavat' a prijímat'
bezpečnostné opatrenia tret'ou stranou“*

*Tretia strana ako vlastník rizík podľa Analýzy rizík vyhlasuje, že pre tieto riziká
prijala bezpečnostné opatrenia. Konkrétna špecifikácia a rozsah
bezpečnostných opatrení Tretej strany tvorí Prílohu č. XY Zmluvy.*

*Tretia strana vyhlasuje, že počas účinnosti Zmluvy bude dodržiavat' všetky
bezpečnostné opatrenia podľa Prílohy č. XY Zmluvy.*

*„ustanovenia o povinnosti informovat’
prevádzkovateľa základnej služby o
kybernetickom bezpečnostnom incidente a o
všetkých skutočnostiach majúcich vplyv na
zabezpečovanie kybernetickej bezpečnosti“*

najmä:

- zadefinovať KBI alebo sa odvolať na ZoKB
- identifikovať formu, obsah a spôsob hlásenia
- sankčný mechanizmus
- ?odplatnosť?

**„ustanovenie o rozsahu, spôsobe a možnosti
vykonávania kontrolných činností a auditu
prevádzkovateľom základnej služby v tretej
strane“**

najmä:

- vymedzenie osôb oprávnených na výkon kontrolných činností a auditu
- spôsob oboznámenia o plánovanej kontrole / audite (lehota, obsah, osoby, miesto výkonu...)
- povinnosti osôb zúčastnených na audite / kontrole

- náklady auditu / kontroly

Komparácia ZoKB a GDPR

ZoKB (§ 19/2)	GDPR (čl. 28)
konkrétne špecifikácia a rozsah bezpečnostných opatrení	primerané technické a organizačné opatrenia
ustanovenie o kontrolných činnostiach a audite	umožnenie auditov a kontrol vykonávaných prevádzkovateľom alebo iným audítorom
podmienky a možnosti zapojenia ďalšieho dodávateľa	podmienky zapojenia ďalšieho sprostredkovateľa
mlčanlivosť	dôvernosť / mlčanlivosť
po ukončení vzťahu previesť alebo zničiť informácie	po ukončení vzťahu vymazať alebo vrátiť osobné údaje

ZoKB (§ 19/2)

dodržiavanie bezpečnostných politík

konkrétny rozsah činností tretej strany

zoznam pracovných rolí tretej strany

povinnosť informovať o KBI

spôsob a forma hlásenia ďalších informácií

sankčný mechanizmus

podmienky a spôsob ukončenia zmluvy

zabezpečenie kontinuity aspoň 5 rokov po ukončení zmluvného vzťahu

ZoITVS

z. č. 95/2019 Z.z. o informačných technológiách
vo verejnej správe a o zmene a doplnení
niektorých zákonov

ZoITVS

FÁZA PRÍPRAVY A OBSTARANIA

ustanovenia k zdrojovému kódu (EUPPL)

plná súčinnosť pri prechode na nového dodávateľa

BEZPEČNOSŤ

bezpečné vývojové prostredie

dokumentácia vývoja vrátane používateľskej dokumentácie a
administrátorskej dokumentácie

mlčanlivosť

dodržiavanie vhodných bezpečnostných mechanizmov

upozornenie na kritické alebo na rizikové časti ISVS

Ďakujem za pozornosť!

spilar@bch.sk