Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI
ŽILINSKEJ UNIVERZITY V ŽILINE

Dodávateľský reťazec

Organizačné opatrenia (Blok II)

Kurz: Manažér kybernetickej bezpečnosti

Ľubomíra Sokolová

KC KYB UNIZA, https://kc.uniza.sk/

kckyb@uniza.sk

NIS 2 ⟶ NOVELA ZÁKONA O KYBERNETICKEJ BEZPEČNOSTI

Novelizuje predošlý zákon o kybernetickej bezpečnosti č. 69/2018 Z.z. a prináša nasledujúce kľúčové zmeny.

- Regulované organizácie a služby
- Bezpečnosť dodávateľského reťazca
- Hlásenie incidentov
- Pokuty
- Vzdelávanie
- Aplikácia bezpečnostných opatrení na základe analýzy rizík
- Koordinované zverejňovanie zraniteľností
- Audit a samohodnotenie
- Certifikácia bezpečnosti IKT produktov a služieb

Riadenie bezpečnosti vo vzťahoch s tretími stranami

Outsourcing ako bežná prax v komerčnej sfére

- Firmy prenášajú **vedľajšie činnosti** na **externých dodávateľov**
- Sústredia sa na svoj **core biznis** – hlavné výkony

Cieľ outsourcingu

- Zvýšiť **efektivitu a flexibilitu**
- Odľahčiť interné kapacity
- Rozhodovanie o efektivite je na **ekonómoch**

Bezpečnostné hľadisko

- Dodávky od tretích strán často zahŕňajú **informačné aktíva**
- **Nový typ rizika pre informačnú bezpečnosť**
- Nutnosť **identifikovať, vyhodnotiť a riadiť riziká**

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Insourcing alebo outsourcing?

Outsourcovať, alebo si ponechať činnosti „doma“?

- Rozhodovanie o outsourcingu musí zahŕňať aj **posúdenie bezpečnosti informačných aktív**.
- Treba zvážiť:
  - ktoré činnosti sú **kritické** a **nevhodné na outsourcing**,
  - aký je dopad na **personálne zloženie a štruktúru** organizácie.

Nie všetky činnosti sú vhodné na outsourcing

- Činnosti a aktíva s **vysokou hodnotou** alebo klasifikované ako **kritické** by mali zostať **vnútorné** (insourcing).
- Prílišné spoliehanie sa na externých dodávateľov môže znížiť kontrolu nad citlivými údajmi.

Zmluvná ochrana informačných aktív je zákonná povinnosť

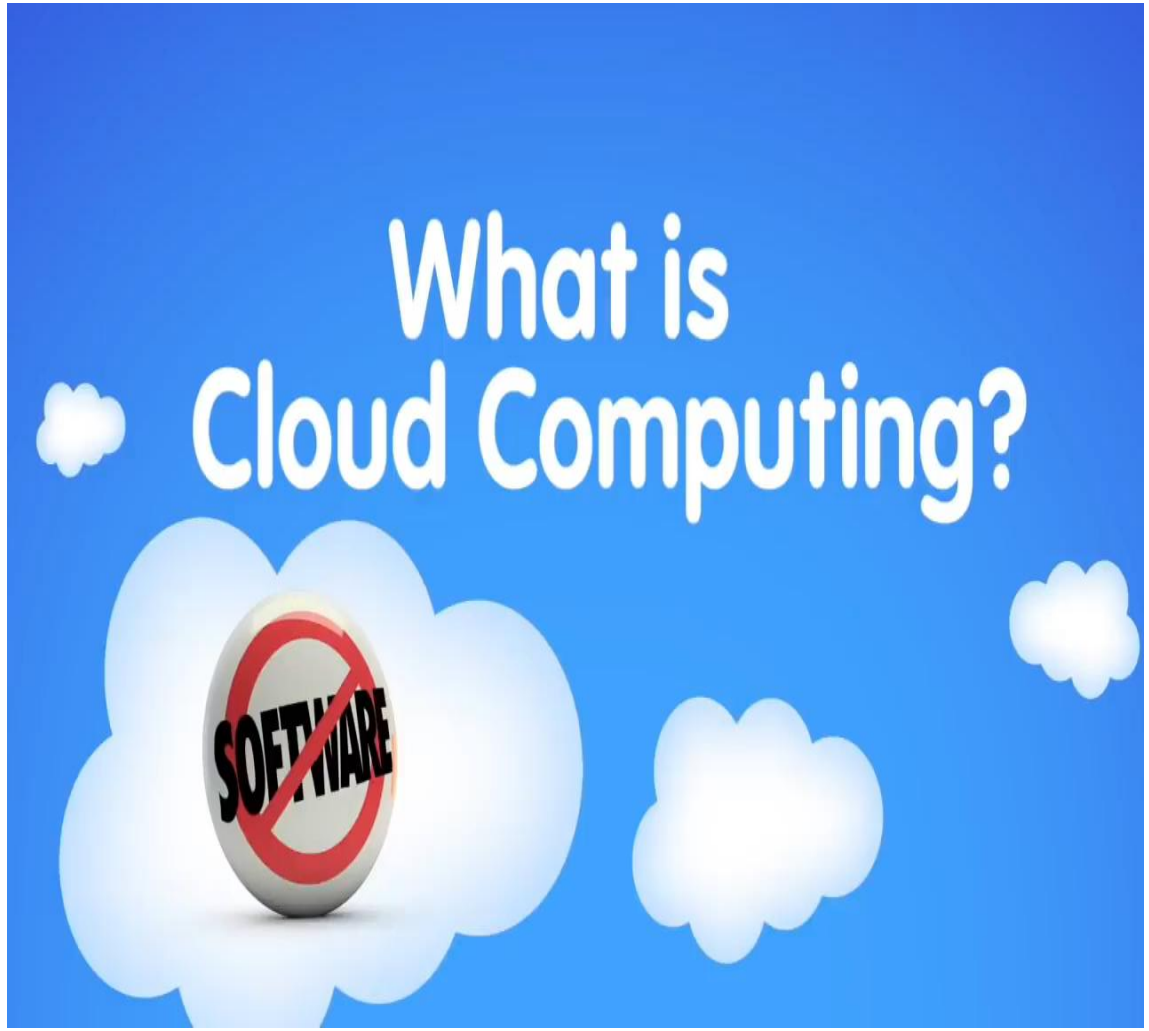
- Vychádza z/zo:
  Zákona o kybernetickej bezpečnosti (č.69/2018 Z.z.)
  Nariadenia GDPR (čl. 28, čl.32)
  Zákona o bankách, technických normách, a iných ...

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Cloudové služby = forma outsourcingu

- Väčšina cloudových služieb sa považuje za dodávateľský spôsob výkonu služieb.
- Podliehajú bezpečnostným požiadavkám

➢ **Pred rozhodnutím o outsourcingu treba:**
  - ➢ Identifikovať klasifikované a citlivé aktíva.
  - ➢ Vyhodnotiť, či outsourcing nezníži ich ochranu.
  - ➢ Vypracovať posúdenie/analýzu rizík a zaviesť kontrolné opatrenia.
  - ➢ Stanoviť jasné pravidlá v zmluve s dodávateľom.



Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Cloud = špecifický typ outsourcingu

- Keď organizácia **neprevádzkuje niečo sama**, ale **zverí to externej firme**, hovoríme o **outsourcingu**. Cloudová služba (napr. IaaS, PaaS, SaaS) je **špeciálna forma outsourcingu v oblasti IT**, ktorá sa vyznačuje týmito znakmi:

Cloudová služba	**Bežný outsourcing**
Beží cez **internet/cloud infraštruktúru**	Môže ísť aj o prenájom ľudí, tímov, techniky
Má **štandardizované rozhrania, samoobslužnosť**	Je často **prispôsobený na mieru**
Poskytovateľ zaručuje **dostupnosť a škálovateľnosť**	Môže byť obmedzený zmluvou a zdrojmi
Účtuje sa ako **služba na báze spotreby** (pay-as-you-go)	Zvyčajne **pevná cena alebo projektové platby**
Môže ísť o **IaaS / PaaS / SaaS**	Môže ísť o **ľudské zdroje, helpdesk, atď.**

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky | Kompetenčné centrum kybernetickej bezpečnosti Žilinskej univerzity v Žiline

Identifikujte riziko skôr, než vyberiete dodávateľa

Dodávatelia môžu získať prístup k citlivým informáciám

Riziká treba identifikovať pred začiatkom spolupráce

Neskorá analýza rizík môže ohroziť organizáciu

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Príklady typov dodávateľov a rizík v KB

Typ dodávateľa	Poskytované služby	Prístup k údajom/systémom	Príklady rizík
Dodávateľ softvérového zabezpečenia	Antivírusy, EDR, firewall, DLP, SIEM	Vysoký	Nesprávna konfigurácia, zber dát mimo EÚ, zraniteľnosti
Penetračný tester / Etický hacker	Testy zraniteľností, simulované útoky	Vysoký / úplný	Zneužitie prístupu, únik testovacích dát
MSSP (Managed Security Service Provider)	Outsourcing bezpečnostného monitoringu (SOC, SIEM, logy)	Veľmi vysoký	Nedostatočný dohľad, oneskorené reakcie, slabé SLA
Konzultant kybernetickej bezpečnosti	Poradenstvo, audit, risk management	Stredný až vysoký	Slabá odbornosť, nesprávne odporúčania
Dodávateľ cloudových služieb	Hosting, úložisko, cloudové platformy	Vysoký	Nedostatočné šifrovanie, prenos dát do tretích krajín
Dodávateľ IAM riešení	Identity and Access Management (prístupy, autentifikácia)	Vysoký	Chyby v prístupových právach, zraniteľné API

Prečo nestačí analyzovať riziko až po výbere dodávateľa?

1. Dodávateľ môže už mať prístup k citlivým údajom

- Po uzavretí zmluvy môže mať dodávateľ prístup k systémom, databázam alebo interným procesom.
- Ak sa až v tomto bode zistí, že dodávateľ nie je dôveryhodný, môže byť **neskoro zabrániť úniku alebo zneužitiu informácií**.
- Odstúpenie od zmluvy môže byť právne a finančne náročné.

2. Vysoké riziká sa často prejavia až pri hlbšej analýze

- Mnohé bezpečnostné riziká nie sú na prvý pohľad zrejmé.
- Až po dôkladnej analýze zistíte, že:
  - dodávateľ nemá zavedené bezpečnostné politiky,
  - má slabé technické zabezpečenie,
  - alebo má prepojenia s rizikovými subjektmi.
- Včasná identifikácia umožňuje prijať kompenzačné opatrenia alebo sa rozhodnúť pre iného dodávateľa.

3. Neseriózni dodávatelia predstavujú hrozbu

- Môžu mať zlú históriu (porušenie zmlúv, úniky údajov, slabé zabezpečenie).
- Môžu zámerne zneužiť získaný prístup – najmä pri práci s osobnými údajmi alebo finančnými informáciami.
- Ich konanie môže viesť k právnej zodpovednosti pre vašu organizáciu (napr. za porušenie GDPR).
- Zlá voľba dodávateľa môže mať dlhodobý dopad na reputáciu a dôveru klientov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Primeranosť posúdenia rizík – rozdiely podľa typu služby a dodávateľa

- Posúdenie rizika musí byť primerané:
  - typu služby,
  - citlivosti zdieľaných informácií,
  - potenciálnemu dopadu na organizáciu.

Nie všetky služby sú rovnaké, napr. z pohľadu citlivosti údajov:

Typ služby / Dodávateľa	Citlivosť údajov	Príklad rizika
Kancelársky materiál	Nízka	Nepotrebné podrobné preverenie
Mzdová agenda (outsourcing HR)	Vysoká	Spracovanie osobných údajov (GDPR)
Výrobca hardvéru	Nízka až stredná	Záleží na použití, často bez prístupu k dátam
Vývojár softvéru pre interný systém	Vysoká	Dlhodobý vplyv na kvalitu, integritu obchodných údajov

Posudzujte riziká **dynamicky**, podľa typu služby, údajov aj očakávaného dopadu.

Financované Európskou úniou NextGenerationEU | PLÁN OBNOVY | MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY | KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Vyhláška NBÚ č. 227/2025 o bezpečnostných opatreniach

§ 5 Riadenie rizík obsahuje

- identifikáciu aktív,
- identifikáciu rizík, ktorej súčasťou je aj opis prijatých a vykonávaných bezpečnostných opatrení,
- analýzu rizík; ak prevádzkovateľ základnej služby disponuje vlastnou bezpečnostnou metodikou, vykoná sa mapovanie na úrovne rizika v súlade so štruktúrou uvedenou v bezpečnostnej metodike zverejnenej na webovom sídle úradu,
- hodnotenie rizík,
- prijatie bezpečnostných opatrení v závislosti od identifikovaných rizík vrátane informácie, ktoré bezpečnostné opatrenia sú prijaté a ktoré bezpečnostné opatrenia nie sú prijaté spolu s odôvodnením,
- preskúmavanie identifikovaných rizík najmenej raz ročne a v závislosti od výsledkov aj aktualizáciu rizík a revíziu prijatých bezpečnostných opatrení.

Vyhláška NBÚ č. 227/2025 o bezpečnostných opatreniach

§ 5 Riadenie rizík

- Súčasťou riadenia rizík je analýza funkčného vplyvu, ktorá pozostáva z hodnotenia vplyvu na činnosť prevádzkovateľa základnej služby spôsobeného krízovým scenárom, ktorý môže zasiahnuť zdroje a aktíva podporujúce procesy prevádzkovateľa základnej služby alebo spôsobiť ohrozenie alebo narušenie kontinuity jeho služieb. Súčasťou analýzy funkčného vplyvu je určenie cieľovej doby obnovy a cieľového bodu obnovy.
- Bezpečnostné opatrenia sa navrhujú, prijímajú a vykonávajú tak, aby ošetrili všetky riziká identifikované v rámci vykonanej analýzy rizík, naplnili požiadavky stratégie kybernetickej bezpečnosti, bezpečnostnej politiky a bezpečnostných opatrení.

Analýzou rizík sa určuje pravdepodobnosť vzniku škodlivej udalosti, ktorá môže byť spôsobená zneužitím existujúcej zraniteľnosti aktíva potenciálnymi hrozbami v spojitosti s existujúcimi bezpečnostnými opatreniami. V rámci analýzy rizík sú identifikované následky pri narušení dôvernosti, integrity alebo dostupnosti aktíva.

- Metodika analýzy rizík - web NBÚ https://www.nbu.gov.sk/metodika-analyzy-rizik/

Zákon č.69/2018 - § 19 Povinnosti prevádzkovateľa základnej služby

Bezpečnosť dodávateľského reťazca

(2) Prevádzkovateľ základnej služby je povinný pri výkone činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby výkonu tejto činnosti; pri uzatvorení zmluvy sa vykonáva analýza rizík. Tretia strana je počas trvania zmluvného vzťahu povinná vykonávať a realizovať bezpečnostné opatrenia v súlade s písomnou zmluvou a týmto zákonom a je povinná podrobiť sa kontrole plnenia týchto opatrení zo strany prevádzkovateľa základnej služby. Ak ide o zmluvu podľa prvej vety uzatvorenú s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu, kontrolu môže vykonávať aj úrad; na tento účel má tretia strana postavenie prevádzkovateľa základnej služby. Uzatvorenie zmluvy podľa prvej vety nesmie brániť v hospodárskej súťaži.

× Zrušiť označenie

(3) Povinnosť uzatvoriť zmluvu podľa odseku 2 neplatí, ak je tretia strana prevádzkovateľom základnej služby, alebo ak je riziko vo vzťahu k činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby prostredníctvom tretej strany nízke.

(4) Prevádzkovateľ základnej služby je povinný informovať v nevyhnutnom rozsahu tretiu stranu o hlásenom kybernetickom bezpečnostnom incidente za predpokladu, že by sa plnenie zmluvy podľa odseku 2 stalo nemožným, ak úrad nerozhodne inak. Povinnosť zachovávať mlčanlivosť tým nie je dotknutá.

(5) Ak prevádzkovateľ základnej služby túto službu poskytuje aj v inom členskom štáte Európskej únie, úrad v súčinnosti s príslušným orgánom tohto členského štátu rozhodne o tom, podľa kritérií ktorého členského štátu bude prevádzkovateľ základnej služby identifikovaný tak, aby bol jednoznačne identifikovaný ako prevádzkovateľ základnej služby aspoň v jednom z týchto členských štátov.

Zákon č.69/2018 - § 19 Povinnosti prevádzkovateľa základnej služby

Bezpečnosť dodávateľského reťazca

- **§ 19 Povinnosti prevádzkovateľa základnej služby -** analyzovať závislosti svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v **dodávateľskom reťazci** a poskytovaných služieb s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu.
- 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.
- **§ 20 Aplikácia bezpečnostných opatrení – q) dodávateľský reťazec**

Bezpečnostné opatrenia sa prijímajú a realizujú na základe analýzy rizík kybernetickej bezpečnosti, ktorá určuje pravdepodobnosť vzniku škodlivej udalosti.

(Prílohač.1 č. k vyhláške č. 227/2025 Z. z.-ROZSAH BEZPEČNOSTNÝCH OPATRENÍ PRE OBLASTI KYBERNETICKEJ BEZPEČNOSTI PODĽA § 20 ODS. 2 ZÁKONA)

Zákon č.69/2018 - § 19 Povinnosti prevádzkovateľa základnej služby

Bezpečnosť dodávateľského reťazca

- Prevádzkovateľ základnej služby je povinný pri výkone prostredníctvom tretej strany, uzatvoriť zmluvu o zabezpečení plnenia bezpečnostných opatrení a notifikačných povinností podľa tohto zákona počas celej doby výkonu tejto činnosti.

- Pri uzatvorení zmluvy sa vykonáva analýza rizík.

- Tretia strana je počas trvania zmluvného vzťahu povinná vykonávať a realizovať bezpečnostné opatrenia v súlade s písomnou zmluvou a zákonom, a je povinná podrobiť sa kontrole plnenia týchto opatrení zo strany prevádzkovateľa základnej služby.

- Ak ide o zmluvu podľa prvej vety uzatvorenú s prevádzkovateľom základnej služby, ktorý prevádzkuje kritickú základnú službu, kontrolu môže vykonávať aj úrad

- Uzatvorenie zmluvy podľa prvej vety nesmie brániť v hospodárskej súťaži.

Zákon č.69/2018 - § 19 Povinnosti prevádzkovateľa základnej služby

Bezpečnosť dodávateľského reťazca

Prevádzkovateľ základnej služby je povinný:

- analyzovať závislosti svojich aktív, informačných systémov, využívaných produktov IKT a služieb IKT tretích strán v dodávateľskom reťazci a poskytovaných služieb s cieľom identifikovať možné dopady kybernetického bezpečnostného incidentu,

- prijať, dodržiavať a vykonávať bezpečnostné opatrenia s prihliadnutím na bezpečnostné metodiky a politiky úradu, najnovšie bezpečnostné trendy, príklady dobrej praxe a medzinárodné normy.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Bezpečnosť dodávateľského reťazca

- Tretia strana, ktorá má významný vplyv pri zabezpečovaní kybernetickej bezpečnosti, má uzatvorenú zmluvu s PZS, ktorý prevádzkuje kritickú základnú službu má postavenie PZS.
- PKZS je povinný úradu hlásiť uzatvorenie zmluvy s takouto treťou stranou a aj jej ukončenie.
- Tretia strana sa zapisuje do registra PZS.
- Tretia strana povinná plniť bezpečnostné opatrenia podľa zákona a podlieha dohľadu zo strany NBÚ.

Vyhláška NBÚ č. 227/2025 o bezpečnostných opatreniach

(6) Podporné aktívum, ktoré súvisí s viacerými primárnymi aktívami, preberá najvyššiu hodnotu zo súvisiacich aktív.

§ 7

(1) Bezpečnostné opatrenia sa navrhujú, prijímajú a vykonávajú tak, aby ošetrili všetky riziká identifikované v rámci vykonanej analýzy rizík, naplnili požiadavky stratégie kybernetickej bezpečnosti, bezpečnostnej politiky a bezpečnostných opatrení podľa § 3 až 6.

(2) Zmluva podľa **§ 19 ods. 2 zákona** obsahuje najmä

a) záväzok dodávateľa na výkon činnosti, ktorá priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa základnej služby (ďalej len „tretia strana“) dodržiavať bezpečnostné politiky prevádzkovateľa základnej služby,

b) vyjadrenie súhlasu tretej strany s uvedenými bezpečnostnými politikami,

c) ustanovenie o rozsahu, spôsobe a možnosti vykonávania kontrolných činností a auditu prevádzkovateľom základnej služby u tretej strany,

d) ustanovenie o povinnosti informovať prevádzkovateľa základnej služby o kybernetickom bezpečnostnom incidente a o skutočnostiach majúcich vplyv na zabezpečovanie kybernetickej bezpečnosti a poskytnúť súčinnosť pri jeho riešení.

(3) Vzor bezpečnostnej dokumentácie a vzor zmluvy podľa § 19 ods. 2 zákona sa zverejnia na webovom sídle úradu.

§ 8

Zmluva podľa **§ 19 ods. 2 zákona** uzatvorená do 31. augusta 2025 ostáva v platnosti najneskôr do doby pôvodne v nej dohodnutej; túto dobu nemožno po 31. auguste 2025 predĺžiť, ak už uzatvorená zmluva nie je v súlade s bezpečnostnými opatreniami podľa § 3 až 7. Týmto ustanovením nie je dotknutý **§ 34b ods. 5 zákona**.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Zmluvná ochrana informačných aktív

- **Zákon o kybernetickej bezpečnosti (69/2018 Z.z.)**
- **Nariadenie GDPR** (čl. 28, čl. 32)

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

GDPR požiadavky a dodávateľský reťazec

- GDPR (Všeobecné nariadenie o ochrane údajov) kladie dôraz na **zodpovednosť prevádzkovateľa aj sprostredkovateľa** pri spracúvaní osobných údajov. To znamená, že ak si firma najme externého dodávateľa (napr. cloudové služby, IT podporu, hosting), nesie zodpovednosť za to, že tento dodávateľ dodržiava primerané bezpečnostné opatrenia na ochranu dát.
- 👉 Prepojenia medzi dodávateľským reťazcom a GDPR:
- **Zodpovednosť za dodávateľov** – Organizácia musí preveriť, či jej partneri a dodávatelia dodržiavajú GDPR (tzv. due diligence).
- **Zmluvné vzťahy** – GDPR vyžaduje uzatvoriť so sprostredkovateľmi *zmluvy o spracúvaní osobných údajov* (DPA), kde sa definujú bezpečnostné opatrenia.
- **Kybernetická bezpečnosť** – Článok 32 GDPR prikazuje zaviesť primerané technické a organizačné opatrenia. To sa vzťahuje aj na dodávateľský reťazec (napr. šifrovanie dát, bezpečný prenos, prístupové práva).
- **Riziká dodávateľského reťazca** – Ak dôjde k úniku údajov cez dodávateľa, zodpovednosť padá aj na firmu, ktorá ho využíva. V praxi sa často rieši cez bezpečnostné audity, certifikácie (ISO 27001) alebo hodnotenie dodávateľov.
- **Incidenty a oznamovanie porušení** – GDPR ukladá povinnosť nahlásiť únik dát do 72 hodín. Ak únik spôsobí dodávateľ, musí o tom okamžite informovať objednávateľa.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

GDPR požiadavky a dodávateľský reťazec

GDPR požiadavka	Ako sa premieta do dodávateľského reťazca	Príklad z praxe
Zodpovednosť prevádzkovateľa (čl. 24, 28)	Firma je zodpovedná aj za svojich dodávateľov, ktorí spracúvajú dáta.	E-shop používa externý cloud – musí preveriť, či cloudový poskytovateľ dodržiava GDPR.
Zmluvy o spracúvaní údajov (DPA)	Povinnosť uzatvoriť so sprostredkovateľom zmluvu s jasne definovanými bezpečnostnými opatreniami.	Firma outsourcuje účtovníctvo – v zmluve sa špecifikuje, ako budú chránené osobné údaje klientov.
Primerané bezpečnostné opatrenia (čl. 32)	Dodávateľ musí zaviesť technické a organizačné opatrenia (šifrovanie, prístupové práva, monitoring).	Hostingová firma musí mať zabezpečené servery proti neoprávnenému prístupu.
Hodnotenie rizík	Prevádzkovateľ musí vyhodnotiť riziká dodávateľského reťazca.	Banka preveruje IT dodávateľov cez bezpečnostný audit pred podpisom zmluvy.
Oznamovanie incidentov (čl. 33)	Dodávateľ je povinný informovať prevádzkovateľa o úniku dát bez zbytočného odkladu.	Ak IT firma zistí únik hesiel, musí okamžite kontaktovať svojho klienta, aby ten stihol nahlásiť porušenie Úradu na ochranu osobných údajov.
Medzinárodné prenosy dát	Dodávatelia mimo EÚ musia dodržiavať špeciálne pravidlá (napr. štandardné zmluvné doložky).	Firma využíva call centrum v Indii – musí mať právne ošetrený prenos dát.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

GDPR požiadavky a dodávateľský reťazec (čl. 28 GDPR – sprostredkovateľ)

- Ak sa má spracúvanie uskutočniť v mene prevádzkovateľa, prevádzkovateľ využíva len sprostredkovateľov poskytujúcich dostatočné záruky na to, že sa prijmú primerané technické a organizačné opatrenia tak, aby spracúvanie spĺňalo požiadavky tohto nariadenia a aby sa zabezpečila ochrana práv dotknutej osoby.

- Sprostredkovateľ nezapojí ďalšieho sprostredkovateľa bez predchádzajúceho osobitného alebo všeobecného písomného povolenia prevádzkovateľa. V prípade všeobecného písomného povolenia sprostredkovateľ informuje prevádzkovateľa o akýchkoľvek zamýšľaných zmenách v súvislosti s pridaním alebo nahradením ďalších sprostredkovateľov, čím sa prevádzkovateľovi dá možnosť namietať voči takýmto zmenám.

GDPR požiadavky a dodávateľský reťazec (čl. 28 GDPR – sprostredkovateľ)

Sprostredkovateľ:

- vykoná všetky požadované opatrenia podľa článku 32(bezpečnosť spracúvania);
- dodržiava podmienky zapojenia ďalšieho sprostredkovateľa;
- po zohľadnení povahy spracúvania v čo najväčšej miere pomáha prevádzkovateľovi vhodnými technickými a organizačnými opatreniami pri plnení jeho povinnosti reagovať na žiadosti o výkon práv dotknutej osoby ustanovených v kapitole III;
- po ukončení poskytovania služieb týkajúcich sa spracúvania na základe rozhodnutia prevádzkovateľa všetky osobné údaje vymaže alebo vráti prevádzkovateľovi a vymaže existujúce kópie, ak právo Únie alebo právo členského štátu nepožaduje uchovávanie týchto osobných údajov.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

GDPR požiadavky a dodávateľský reťazec (čl. 28 GDPR – sprostredkovateľ)

- Sprostredkovateľ poskytne prevádzkovateľovi všetky informácie potrebné na preukázanie splnenia povinností stanovených v tomto článku a umožní audity, ako aj kontroly vykonávané prevádzkovateľom alebo iným audítorom, ktorého poveril prevádzkovateľ, a prispieva k nim.
- Sprostredkovateľ bezodkladne informuje prevádzkovateľa, ak sa podľa jeho názoru pokynom porušuje toto nariadenie alebo iné právne predpisy Únie alebo členského štátu týkajúce sa ochrany údajov.

Ak sprostredkovateľ zapojí do vykonávania osobitných spracovateľských činností v mene prevádzkovateľa ďalšieho sprostredkovateľa, tomuto ďalšiemu sprostredkovateľovi sa prostredníctvom zmluvy alebo iného právneho aktu podľa práva Únie alebo práva členského štátu uložia rovnaké povinnosti ochrany údajov, ako sa stanovujú v zmluve alebo inom právnom akte uzatvorenom medzi prevádzkovateľom a sprostredkovateľom, a to predovšetkým poskytnutie dostatočných záruk na vykonanie primeraných technických a organizačných opatrení.

GDPR požiadavky a dodávateľský reťazec (čl. 28 GDPR – sprostredkovateľ)

- Dodržiavanie schváleného kódexu (napr. bankový sektor, advokáti) správania sa môže použiť ako prvok na preukázanie dostatočných záruk.

Článok 32 GDPR - Bezpečnosť spracúvania

Prevádzkovateľ a sprostredkovateľ prijmú primerané technické a organizačné opatrenia

a) pseudonymizáciu a šifrovanie;

b) schopnosť zabezpečiť trvalú dôvernosť, integritu, dostupnosť a odolnosť systémov spracúvania a služieb;

c) schopnosť včas obnoviť dostupnosť a prístup v prípade fyzického alebo technického incidentu;

d) proces pravidelného testovania, posudzovania a hodnotenia účinnosti technických a organizačných opatrení na zaistenie bezpečnosti spracúvania.

Financované Európskou úniou NextGenerationEU
PLÁN OBNOVY
MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY
KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Otázky v súvislosti s dodávateľským reťazcom

- Ktoré činnosti by ste určite neoutsourcovali vo vlastnej organizácii?
- Ako by ste zabezpečili ochranu citlivých údajov, ak musíte zapojiť externého partnera?
- Čo musíte splniť podľa novely zákona pri výbere nového dodávateľa?
- Čo je povinný prevádzkovateľ základnej služby pri výkone činnosti prostredníctvom tretej strany uzatvoriť, pokiaľ to priamo súvisí s dostupnosťou, dôvernosťou a integritou prevádzky sietí a informačných systémov prevádzkovateľa ?
- Aké náležitosti má obsahovať zmluva v zmysle Vyhlášky NBÚ č. 227/2025 o bezpečnostných opatreniach?

Financované Európskou úniou
NextGenerationEU

PLÁN OBNOVY

MINISTERSTVO INVESTÍCIÍ, REGIONÁLNEHO ROZVOJA A INFORMATIZÁCIE SLOVENSKEJ REPUBLIKY

KOMPETENČNÉ CENTRUM KYBERNETICKEJ BEZPEČNOSTI ŽILINSKEJ UNIVERZITY V ŽILINE

Ďakujem za pozornosť

Organizačné opatrenia. Dodávateľský reťazec Blok II

Kurz: Manažér kybernetickej bezpečnosti

Ing. Ľubomíra Sokolová, PhD.

KC KYB UNIZA, https://kc.uniza.sk/

kckyb@uniza.sk