(Návrh)

Vyhláška
Štatistického úradu Slovenskej republiky

z ... 2026,

ktorou sa upravujú podrobnosti o postupe člena národného štatistického systému pri poskytovaní a ochrane dôverných štatistických údajov na vedecký účel

Štatistický úrad Slovenskej republiky (ďalej len „úrad“) podľa § 74 písm. f) zákona č. .../2026 Z. z. o oficiálnej štatistike a o zmene a doplnení niektorých zákonov (zákon o oficiálnej štatistike) ustanovuje:

§ 1
Predmet úpravy

(1) Táto vyhláška upravuje podrobnosti o postupe člena národného štatistického systému pri poskytovaní a ochrane dôverných štatistických údajov na vedecký účel [§ 55 ods. 2 písm. a) prvý bod zákona o oficiálnej štatistike] vrátane opatrení na ochranu kybernetickej bezpečnosti a informačnej bezpečnosti, ktoré je povinný dodržiavať výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby.[1])

(2) Táto vyhláška sa primerane vzťahuje aj na postup úradu a iného člena národného štatistického systému, ak iný člen národného štatistického systému poskytuje dôverné štatistické údaje do informačného systému úradu na realizáciu zmluvy o poskytnutí dôverných štatistických údajov medzi iným členom národného štatistického systému a výskumným subjektom [§ 55 ods. 1 písm. d) zákona o oficiálnej štatistike] spôsobom podľa § 56 ods. 5 písm. b) alebo písm. c) zákona o oficiálnej štatistike.

§ 2
Žiadosť o poskytnutie dôverných štatistických údajov na vedecký účel

(1) Žiadosť o poskytnutie dôverných štatistických údajov na vedecký účel (ďalej len „žiadosť o poskytnutie dôverných štatistických údajov“) sa predkladá členovi národného štatistického systému, ktorý spracúva požadované dôverné štatistické údaje, listinne alebo elektronicky, a to výlučne na formulároch, ktorých vzory úrad zverejní na svojom webovom sídle.

---

[1]) § 3 ods. 2 zákona č. 69/2018 Z. z. v znení zákona č. 366/2024 Z. z.

(2) Člen národného štatistického systému poskytuje dôverné štatistické údaje na vedecký účel podľa
   a) individuálnej požiadavky výskumného subjektu,
   b) ako dataset pripravený na opakované použitie určený bližšie vopred neurčenému počtu výskumných subjektov na základe vyhodnotenia opakujúcich sa požiadaviek používateľov oficiálnej štatistiky.

§ 3
Predpoklady poskytnutia dôverných štatistických údajov na vedecký účel

(1) Výskumný subjekt, ktorému zákon alebo právny predpis cudzieho štátu priamo neustanovuje povinnosť vykonávať výskum alebo vývoj, alebo ktorý nie je analytickou jednotkou, preukazuje spôsobilosť vykonávať výskum alebo vývoj podľa osobitného predpisu[2]) alebo vecne rovnakú spôsobilosť podľa právneho poriadku štátu, v ktorom má svoje sídlo (ďalej len „spôsobilosť vykonávať výskum“)
   a) predložením platného osvedčenia o spôsobilosti vykonávať výskum vydaným Ministerstvom školstva, vedy, výskumu a mládeže Slovenskej republiky alebo príslušným orgánom cudzieho štátu,
   b) zaradením výskumného subjektu v zozname uznaných výskumných zariadení,[3]) ktorý zverejňuje Európska komisia (Eurostat) podľa osobitného predpisu[4]) a uverejňuje ho na svojej webovej stránke,
   c) predložením oprávnenia vydaného príslušným orgánom cudzieho štátu pôsobiť ako vysoká škola alebo ako vedecká inštitúcia alebo označením právneho predpisu cudzieho štátu, z ktorého vyplýva takéto oprávnenie, alebo
   d) u výskumného subjektu, ktorý objektívne nemôže preukázať spôsobilosť vykonávať výskum podľa písm. a) až c), predložením
      1. štatútu alebo iného dokumentu, ktorý preukazuje, že účelom výskumného zariadenia je aj výskum alebo vývoj,
      2. dokumentácie, ktorá preukazuje že výskumný subjekt uskutočňuje hodnotný výskum a dáva ho k dispozícii verejnosti; dokumentáciou sú najmä dostupné zoznamy publikácií a výskumných projektov, na ktorých sa výskumný subjekt zúčastnil,
      3. dokumentu, ktorý ustanovuje alebo z neho vyplýva, že výskumný subjekt:
         3a. má právnu subjektivitu alebo má postavenie organizačnej zložky právnickej osoby alebo fyzickej osoby - podnikateľa,
         3b. je nezávislý a autonómny pri formulovaní vedeckých záverov a oddelený od politických oblastí subjektu, do ktorého je organizačne začlenený alebo ktorý je jeho zriaďovateľom.

---

[2]) § 16 ods. 1 a 26a zákona č. 172/2005 Z. z. v znení neskorších predpisov.
[3]) Čl. 4 ods. 5 nariadenia Komisie (EÚ) č. 557/2013 zo 17. júna 2013 , ktorým sa vykonáva nariadenie Európskeho parlamentu a Rady (ES) č. 223/2009 o európskej štatistike, pokiaľ ide o prístup k dôverným údajom na vedecký účel, a ktorým sa zrušuje nariadenie (ES) č. 831/2002 (Ú. v. EÚ L 164, 18.6.2013).
[4]) Nariadenie Komisie (EÚ) č. 557/2013.

(2) Výskumný subjekt preukáže členovi národného štatistického systému uskutočňovanie výskumu alebo vývoja
   a) identifikáciou výskumného projektu, projektu vývoja, výskumnej úlohy alebo vývojovej úlohy, dizertačnej práce alebo habilitačnej práce (ďalej len „vedecký projekt“), na ktorého uskutočnenie sú dôverné štatistické údaje nevyhnutné,
   b) písomným potvrdením o doktorandskom štúdiu študenta, pre ktorého výskumný subjekt požaduje dôverné štatistické údaje na vypracovanie dizertačnej práce,
   c) informáciou o využití požadovaných dôverných štatistických údajov,
   d) uvedením očakávaných výstupov z výskumu (napríklad publikácie, odborné články alebo príspevky na konferencie).

(3) Výskumný subjekt preukáže členovi národného štatistického systému analytickú činnosť označením
   a) ustanovení právneho predpisu alebo označením platného uznesenia vlády Slovenskej republiky, ktorý jednoznačne určuje alebo z ktorého jednoznačne vyplýva úloha spracúvať požadované dôverné štatistické údaje a
   b) materiálu alebo iného výstupu, pri ktorého spracovaní je nutné použiť dôverné štatistické údaje.

(4) Člen národného štatistického systému posudzuje spôsobilosť výskumného subjektu zabezpečiť plnenie opatrení na ochranu poskytovaných dôverných štatistických údajov (ďalej len „spôsobilosť chrániť údaje“)
   a) posúdením odpovedí výskumného subjektu uvedených v dotazníku kybernetickej bezpečnosti a informačnej bezpečnosti a písomných dokumentov, ktoré výskumný subjekt v dotazníku označil; vzor formulára dotazníka zverejní úrad na svojom webovom sídle a výskumný subjekt ho prikladá k žiadosti podpísaný štatutárnym orgánom alebo osobou zodpovednou za politiku informačnej bezpečnosti a kybernetickej bezpečnosti, a to spolu s dokumentmi, ktoré v dotazníku označil,
   b) posúdením ďalších verejne dostupných údajov, ktoré preukazujú dodržiavanie opatrení na zabezpečenie kybernetickej bezpečnosti a informačnej bezpečnosti prijatých výskumným subjektom podľa § 7,
   c) vyhodnotením informácií o plnení zmlúv uzavretých s výskumným subjektom na poskytnutie dôverných štatistických údajov v minulosti.

(5) Člen národného štatistického systému upustí pri podaní žiadosti o poskytnutie dôverných štatistických údajov na vedecký účel od posudzovania spôsobilosti chrániť údaje, ak
   a) výskumný subjekt požaduje poskytnutie dôverných štatistických údajov výlučne sprístupnením vo výskumnom dátovom centre,
   b) výskumný subjekt je zaradený v aktuálnom zozname uznaných výskumných zariadení, ktorý vedie Európska komisia (Eurostat),
   c) výskumný subjekt je prevádzkovateľom základnej služby,
   d) od uzavretia inej zmluvy s výskumným subjektom neuplynuli viac ako dva roky, alebo

e) ide o žiadosť výskumného subjektu o predĺženie poskytovania dôverných štatistických údajov podľa už uzavretej zmluvy s tým istým členom národného štatistického systému,

(6) Pri overovaní spôsobilosti vykonávať výskum a vývoj, existencie vedeckého účelu a spôsobilosti chrániť údaje spôsobom určeným v odsekoch 2 až 4 je možné požadované dokumenty a informácie poskytnúť aj uvedením platnej internetovej adresy, na ktorej sú požadované dokumenty alebo informácie verejne dostupné; podmienkou uznania tohto spôsobu preukázania splnenia predpokladov je dôveryhodnosť webového sídla.

(7) Žiadosť o poskytnutie dôverných štatistických údajov sa podáva v slovenskom jazyku.

(8) Informatívne znenie vzorovej žiadosti o poskytnutie dôverných štatistických údajov a dotazníka kybernetickej bezpečnosti a informačnej bezpečnosti v anglickej mutácii zverejní úrad na svojom webovom sídle.

(9) Ak je žiadosť neúplná alebo nezrozumiteľná alebo k nej nie sú priložené doklady, ktoré preukazujú splnenie predpokladov na poskytnutie dôverných štatistických údajov, člen národného štatistického systému vyzve výskumný subjekt na zmenu alebo doplnenie žiadosti o poskytnutie dôverných štatistických údajov.

§ 4
Zmluva o poskytnutí dôverných štatistických údajov na vedecký účel

(1) Zmluva vrátane všetkých príloh sa vyhotovuje v dvoch rovnopisoch.

(2) Zmluva obsahuje najmä:
a) označenie a identifikačné údaje člena národného štatistického systému a výskumného subjektu,
b) meno, priezvisko a funkciu štatutárneho orgánu člena národného štatistického systému a výskumného subjektu,
c) vymedzenie vedeckého projektu, na ktorý sa požaduje poskytnutie dôverných štatistických údajov,
d) doba podľa § 56 ods. 8 alebo ods. 9 zákona o oficiálnej štatistike, po ktorú je možné dôverné štatistické údaje spracovávať,
e) termín poskytnutia dôverných štatistických údajov,
f) meno, priezvisko, pracovné zaradenie a kontaktné údaje kontaktnej osoby a názov organizačného útvaru výskumného subjektu, v ktorom je kontaktná osoba zaradená,
g) záväzok výskumného subjektu oznámiť písomne členovi národného štatistického systému do piatich pracovných dní po uzavretí zmluvy mená, priezviská, pracovné zaradenie, identifikátory fyzickej osoby podľa zákona o e-Governmente a kontaktné údaje výskumných pracovníkov, ktorí uskutočňujú vedecký účel výskumného subjektu, na ktoré sa požaduje poskytnutie dôverných štatistických údajov,

h) meno, priezvisko, kontaktné údaje zamestnanca člena národného štatistického systému určeného na vybavovanie žiadosti,
i) spôsob prístupu k dôverným štatistickým údajom na vedecký účel podľa § 56 ods. 5 zákona o oficiálnej štatistike,
j) poučenie o záväzku mlčanlivosti osôb uvedených v písmene f) a g) a vymedzenie povinností výskumného subjektu ako zmluvnej strany v prípade ohrozenia alebo porušenia štatistickej dôvernosti pri spracúvaní poskytnutých dôverných štatistických údajov,
k) záväzok výskumného subjektu
   1. použiť sprístupnené dôverné štatistické údaje výlučne na účel, ktorý je vymedzený výskumnou úlohou počas doby jej plnenia,
   2. nespájať poskytnuté dôverné štatistické údaje s inými mikroúdajmi s cieľom identifikovať štatistickú jednotku,
   3. neposkytovať dôverné štatistické údaje tretím stranám,
   4. zverejňovať len také výsledky výskumu alebo vývoja, ktoré neobsahujú poskytnuté dôverné štatistické údaje,
   5. zničiť nenávratne poskytnuté dôverné štatistické údaje po skončení doby ich oprávneného spracovávania formou likvidácie dohodnutou v zmluve,
l) záväzok výskumného subjektu, ak nejde o poskytovanie dôverných štatistických údajov vo výskumnom dátovom centre, dodržiavať vlastné opatrenia a právnymi predpismi ustanovené opatrenia na zabezpečenie kybernetickej bezpečnosti a informačnej bezpečnosti použitých pri spracúvaní poskytnutých dôverných štatistických údajov na úrovni, ktorá vyplýva z údajov uvedených v žiadosti, v žiadosti o zápis do zoznamu uznaných výskumných zariadení vedenom Eurostatom alebo v žiadosti, na základe ktorej výskumný subjekt uzavrel s členom národného štatistického systému najviac pred dvoma rokmi inú zmluvu,
m) záväzok výskumného subjektu dodržiavať pravidlá práce vo výskumnom dátovom centre, ktoré sú prílohou zmluvy,
n) záväzok výskumného subjektu, ak nejde o poskytovanie dôverných štatistických údajov vo výskumnom dátovom centre, poskytnúť členovi národného štatistického systému na vyžiadanie v lehote určenej členovom národného štatistického systému informáciu o prvom aj opakovanom zverejnení každého výstupu z výskumu, vývoja alebo analytickej činnosti, na ktorého tvorbu boli použité dôverné štatistické údaje poskytnuté podľa zmluvy (napríklad webová adresa, na ktorej je výstup zverejnený, názov a ISBN tlačenej publikácie); tento záväzok sa nevzťahuje na informáciu poskytnutú výskumným subjektom v žiadosti,
o) záväzok člena národného štatistického systému oboznámiť osoby uvedené v písmene f) a g) s pokynmi pre prácu s dôvernými štatistickými údajmi na vedecký účel podľa prílohy zmluvy,
p) záväzok člena národného štatistického systému vytvoriť podmienky na plnohodnotné využitie výskumného dátového centra, ak sa údaje sprístupňujú týmto spôsobom,
q) záväzok člena národného štatistického systému poskytnúť súčinnosť zamestnancov pri spracúvaní sprístupnených štatistických údajov,

r) poučenie o možnosti člena národného štatistického systému stíhať výskumný subjekt za porušenie štatistickej dôvernosti pri spracúvaní poskytnutých dôverných štatistických údajov ako správny delikt,
s) štruktúru poskytovaných dôverných štatistických údajov spolu s metadátovým popisom, ktorá je prílohou zmluvy,
t) poučenie o záväzku mlčanlivosti výskumných pracovníkov a ďalších fyzických osôb, ktoré sa pri realizácii zmluvy na strane žiadateľa majú možnosť oboznámiť s poskytnutými dôvernými štatistickými údajmi všetkých osôb,
u) povinnosti výskumného subjektu v prípade ohrozenia alebo porušenia štatistickej dôvernosti pri spracúvaní poskytnutých dôverných štatistických údajov,
v) ustanovenia o zmene zmluvy, skončení zmluvy, o riešení sporov a spôsobe vzájomnej komunikácie pri realizácii zmluvy.

(3) Člen národného štatistického systému môže uzatvoriť dvojjazyčnú zmluvu aj v anglickom jazyku len s výskumným subjektom, ktorý nemá sídlo alebo miesto podnikania v Slovenskej republike, pričom v prípade vzniku nejasností alebo rozporov platí znenie zmluvy v slovenskom jazyku. Vyhotovenie návrhu zmluvy v anglickom jazyku zabezpečí člen národného štatistického systému.

(4) Ak sa v priebehu platnosti zmluvy zmení kontaktná osoba alebo osoba výskumného pracovníka, alebo ak sa zmenia údaje podľa odseku 1 písm. f) a g) o kontaktnej osobe alebo o výskumnom pracovníkovi, výskumný subjekt je povinný tieto skutočnosti oznámiť členovi národného štatistického systému v termíne a spôsobom určeným v zmluve.

(5) Termín poskytnutia dôverných štatistických údajov môže byť určený aj dodatočne dohodou kontaktnej osoby a zamestnanca člena národného štatistického systému určeného na vybavenie žiadosti a to najmä z prevádzkovo-technického dôvodu alebo z dôvodu, že údaje bude mať člen národného štatistického systému k dispozícii v budúcnosti. V zmluve je možné určiť aj viac termínov poskytovania dôverných štatistických údajov, ak sa údaje poskytujú po častiach alebo sa poskytujú aktualizované hodnoty tých istých údajov.

§ 6
Výskumné dátové centrum

(1) Výskumné dátové centrum Štatistického úradu Slovenskej republiky (ďalej len „výskumné dátové centrum“) úrad prevádzkuje výlučne na poskytovanie dôverných štatistických údajov na vedecký účel.

(2) Člen národného štatistického systému navrhne výskumnému subjektu sprístupnenie dôverných štatistických údajov vo výskumnom dátovom centre, najmä ak výskumný subjekt požaduje od člena národného štatistického systému taký objem údajov, pre ktorý nie je možné realizovať proces prípravy z dôvodu zvýšenej administratívnej záťaže

alebo z dôvodu, že pri poskytovaní dôverných štatistických údajov na vedecký účel iným spôsobom nie je možné dodržať metodiku procesu prípravy.

(3) Úrad je oprávnený vykonať po skončení spracovania poskytnutých dôverných štatistických údajov kontrolu výstupov spracovaných pracovníkom výskumného subjektu a ak zistí, že môžu viesť k porušeniu štatistickej dôvernosti, upraví ich a pracovníkovi výskumného subjektu poskytne na ďalšiu činnosť. Ak nie je možné výstupy podľa prvej vety upraviť tak, aby neporušovali štatistickú dôvernosť, úrad ich výskumnému subjektu neposkytne, pričom ho o tejto skutočnosti informuje. Výskumnému subjektu je v takom prípade umožnená ďalšia práca vo výskumnom dátovom centre s cieľom prípravy nových výstupov.

(4) Podrobnosti o prevádzke výskumného dátového centra a pravidlá práce s dôvernými štatistickými údajmi vo výskumnom dátovom centre upravuje prevádzkový poriadok; úrad oboznámi pracovníka výskumného subjektu s prevádzkovým poriadkom pred začatím práce vo výskumnom dátovom centre.

§ 7
Opatrenia podľa § 56 ods. 3 písm. g) zákona

Opatrenia na ochranu kybernetickej bezpečnosti a informačnej bezpečnosti, ktoré je povinný dodržiavať výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby,[5]) pri spracúvaní dôverných štatistických údajov na vedecký účel sprístupnených

a) odovzdaním súboru dôverných štatistických údajov spracovaných v procese prípravy na zabezpečenom technickom nosiči alebo zabezpečeným prenosom údajov podľa § 56 ods. 5 písm. b) zákona sú uvedené v prílohe č. 1,
b) prostredníctvom systému vzdialeného prístupu k dôverným štatistickým údajom podľa § 56 ods. 5 písm. c) zákona sú uvedené v prílohe č. 2.

§ 8
Účinnosť

Táto vyhlášky nadobúda účinnosť 1. januára 2027 okrem § 8 písm. b), ktoré nadobúda účinnosť 1. januára 2030.

Martin Nemky, v. r.

[5]) § 3 ods. 2 zákona č. 69/2018 Z. z. v znení zákona č. 366/2024 Z. z.

Príloha č. 1
k vyhláške č. .../2026 Z. z.

OPATRENIA
NA OCHRANU KYBERNETICKEJ BEZPEČNOSTI A INFORMAČNEJ BEZPEČNOSTI PRI SPRÍSTUPNENÍ DÔVERNÝCH ŠTATISTICKÝCH ÚDAJOV NA VEDECKÝ ÚČEL NA ZABEZPEČENOM TECHNICKOM NOSIČI ALEBO ZABEZPEČENÝM PRENOSOM ÚDAJOV

Položka	**Bezpečnostné opatrenia pre organizáciu a riadenie informačnej bezpečnosti a kybernetickej bezpečnosti prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:**
1.	je určená osoba zodpovedná za riadenie prístupu používateľov do siete a k informačnému systému a za prideľovanie a odoberanie prístupových práv používateľom, ich evidenciu a vedenie prevádzkových záznamov o každom prístupe do siete a informačného systému podľa príslušnej bezpečnostnej politiky
2.	je definovaná a schválená štruktúra pre zavedenie, prevádzku a riadenie kybernetickej bezpečnosti vrátane pridelenia úloh, rolí ako aj určenie zodpovedností podľa právomocí na schvaľovanie bezpečnostných opatrení, dohľad, kontrolu, audit a vzdelávanie
3	je definovaný a zavedený systém vzdelávania a preškoľovania pre všetky roly týkajúce sa kybernetickej bezpečnosti
4.	je uplatnená zásada najnižších privilégií, podľa ktorej sú každému používateľovi obmedzené privilégiá v najväčšom rozsahu potrebnom na splnenie pridelených úloh
5.	je uplatnená zásada oddeľovania zodpovedností, podľa ktorej žiaden používateľ nemá oprávnenie upravovať alebo používať aktíva prevádzkovateľa základnej služby bez autorizácie alebo overenia identity
6.	zamestnanci prevádzkovateľa základnej služby a zamestnanci tretích strán pri zmene alebo pri ukončení pracovného pomeru, zmluvy alebo obdobného zmluvného vzťahu preukázateľným spôsobom vracajú prevádzkovateľovi základnej služby všetky aktíva, ktoré mali zverené
7.	je definovaný systém reakcie na kybernetické bezpečnostné incidenty
	Bezpečnostné opatrenia pre správu zraniteľností a kybernetických hrozieb prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:

8.	je zabezpečená informovanosť o identifikovaných kybernetických hrozbách s cieľom prijať primerané bezpečnostné opatrenia vrátane kybernetických hrozieb špecifických pre informačné a komunikačné technológie a operačné technológie
9.	sú získavané informácie o zraniteľnostiach používaných informačných systémov vrátane hodnotenia, do akej miery sú tieto systémy zraniteľné a prijímania vhodných opatrení na ich mitigáciu
	Bezpečnostné opatrenia pre správu aktív a riadenie kybernetických hrozieb a rizík prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
10.	zamestnanci prevádzkovateľa základnej služby a zamestnanci tretích strán pri zmene alebo pri ukončení pracovného pomeru, zmluvy alebo obdobného zmluvného vzťahu preukázateľným spôsobom vracajú prevádzkovateľovi základnej služby všetky aktíva, ktoré mali zverené
	Bezpečnostné opatrenia pre riadenie udalostí a kybernetických bezpečnostných incidentov prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
11.	je definovaný systém reakcie na kybernetické bezpečnostné incidenty
12.	poznatky získané z riešených kybernetických bezpečnostných incidentov sú preukázateľne zohľadnené v procese riadenia kybernetickej bezpečnosti
13.	v prípade kybernetického bezpečnostného incidentu sú dodržiavané všetky stanovené bezpečnostné opatrenia a postupy
14.	sú definované a pravidelne, aspoň raz ročne testované pravidlá pre izoláciu kritických komponentov sietí, informačných systémov a operačných technológií počas kybernetického bezpečnostného incidentu; o vykonaní testovania sa vyhotovuje záznam, ktorý sa uchováva najmenej na obdobie od ukončenia posledného auditu do ukončenia nasledujúceho auditu alebo samohodnotenia
	Bezpečnostné opatrenia pre riadenie kontinuity činností, zálohovanie, obnovu systémov po havárii a krízové riadenie prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
15.	infraštruktúra sietí, informačných systémov a operačných technológií je zriadená s dostatočnou redundanciou
	Bezpečnostné opatrenia pre bezpečnosť pri nadobúdaní, vývoji a údržbe siete, informačných systémov, aplikácií a konfigurácií prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
16.	sú prijaté opatrenia na zabránenie straty, poškodenia, krádeže alebo kompromitácie aktív a prerušeniu prevádzky
17.	prístup k zdrojovému kódu, vývojovým technológiám a softvérovým knižniciam na čítanie a zápis je riadený
18.	sú prijaté bezpečnostné opatrenia s požadovanými bezpečnostnými nastaveniami tak, aby konfigurácia technických prostriedkov, programových prostriedkov, služieb a sietí nebola zmenená neoprávnenými osobami
19.	sú určené a aplikované základné parametre pre bezpečné konfigurácie
20.	sú pri vývoji alebo získavaní aplikácií identifikované a naplnené relevantné požiadavky na kybernetickú bezpečnosť

21.	je zaručený bezpečný návrh, inštalácia a prevádzka sietí, informačných systémov a operačných technológií v rámci životného cyklu
22.	sú riadené, monitorované a kontrolované činnosti súvisiace s vývojom programových prostriedkov a informačných systémov, ktoré sú dodávané treťou stranou
	Bezpečnostné opatrenia pre postupy posudzovania účinnosti opatrení, riadenie súladu a kontrolné činnosti prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
23.	riadenie kybernetickej bezpečnosti je nezávisle prehodnocované v plánovaných intervaloch alebo pri významných zmenách procesov alebo technológií
24.	sú definované pravidlá pre výkon auditných činností a kontrolných činností v oblasti kybernetickej bezpečnosti
	Bezpečnostné pravidlá pre kryptografické opatrenia a zásady používania kryptografie prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
25.	nastavením pravidiel pre použitie vhodných kryptografických metód je obmedzené potenciálne narušenie dôvernosti informácií vrátane osobných údajov a sú dodržiavané požiadavky vyplývajúce zo všeobecne záväzných právnych predpisov, požiadavky vyplývajúce zo zmlúv alebo v prípade certifikovaného subjektu normatívne požiadavky týkajúce sa kybernetickej bezpečnosti
	Bezpečnostné pravidlá pre bezpečnosť a spôsobilosti ľudských zdrojov prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
26.	sú určené pravidlá pre zaradenie osôb do jednotlivých pracovných rolí
27.	v pracovných zmluvách, zmluvách v súvislosti s iným obdobným pracovnoprávnym vzťahom alebo iných súvisiacich dokumentoch sú uvedené zodpovednosti za kybernetickú bezpečnosť pre všetky pracovné roly je poskytované primerané vzdelávanie, aby štatutárny orgán prevádzkovateľa základnej služby, zamestnanci prevádzkovateľa základnej služby a tretie strany mali primerané povedomie o kybernetickej bezpečnosti v oblasti informačných a operačných technológií; súčasťou školení sú aj praktické simulácie a cvičenia reakcie na kybernetické bezpečnostné incidenty
28.	zamestnanci prevádzkovateľa základnej služby a tretie strany sú preukázateľne oboznámení s bezpečnostnými politikami
29.	sú formalizované disciplinárne procesy voči zamestnancom prevádzkovateľa základnej služby, ktorí sa dopustili porušenia ustanovení bezpečnostných politík prevádzkovateľa základnej služby
30.	sú určené, zdokumentované a pravidelne, najmenej raz za dva roky, preskúmavané a podpisované dohody o mlčanlivosti, ktoré odrážajú potreby prevádzkovateľa základnej služby pre zachovanie dôvernosti
31.	ak zamestnanci pracujú na diaľku, sú prijaté bezpečnostné opatrenia na ochranu informácií, ku ktorým sa pristupuje, ktoré sa spracúvajú alebo ktoré sa uchovávajú mimo priestorov prevádzkovateľa základnej služby

32.	sa používa viacfaktorové overovanie pre vzdialený prístup
	Bezpečnostné pravidlá pre správu identít a prístupov prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
33.	pri riadení prístupov k sieťam a informačným systémom sú využívané technológie na správu a overovanie identity používateľa pred začiatkom jeho aktivity v rámci siete a informačného systému a technológie na riadenie prístupových oprávnení, prostredníctvom ktorých je riadený prístup k jednotlivým aplikáciám a údajom, prístup na čítanie údajov a zápis údajov a na zmeny oprávnení a prostredníctvom ktorých sa zaznamenáva použitie prístupových oprávnení
34.	je zaručené riadenie jednoznačných identifikátorov používateľov a systémov vrátane prístupových práv a oprávnení používateľských účtov a systémových účtov, počas celého životného cyklu identít
35.	je zavedené riadenie prístupov na základe rolí a zásady najnižších oprávnení pre používateľov
36.	všetky prístupy do sietí, informačných systémov a operačných technológií z nedôveryhodných zdrojov sú riadené a monitorované
	Bezpečnostné pravidlá pre bezpečnosť pri prevádzke sietí a informačných systémov prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
37.	sa zabraňuje úniku informácií zo zariadení, ktoré sa majú zlikvidovať alebo opätovne použiť; všetky prvky zariadení obsahujúce pamäťové médiá sa kontrolujú, čím sa zabezpečí, že informácie a licencovaný softvér sú bezpečne zmazané alebo prepísané ešte pred vyradením alebo opätovným použitím zariadení
	Bezpečnostné pravidlá pre ochranu proti škodlivému kódu a nežiaducemu obsahu prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
38.	je zavedená ochrana proti škodlivému kódu, ktorá je podporovaná primeraným budovaním povedomia používateľov
39.	je zaručená pravidelná aktualizácia sietí, informačných systémov a operačných technológií s cieľom zabezpečiť minimálne narušenie bežnej prevádzky
	Bezpečnostné pravidlá pre systémovú bezpečnosť, sieťovú bezpečnosť a komunikačnú bezpečnosť prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
40.	na informačné systémy, siete a technické prostriedky, ktoré spracúvajú, uchovávajú alebo prenášajú chránené informácie, podľa klasifikácie informácií, sa aplikujú opatrenia na prevenciu úniku informácií vrátane zohľadnenia proprietárnych protokolov a dátových tokov; identifikácia vybraných informácií prebieha pomocou klasifikácie informácií
41.	siete a technické prostriedky sietí sa zabezpečujú, spravujú a kontrolujú s cieľom chrániť informácie v informačných systémoch, programových prostriedkoch a mobilných aplikáciách
	Bezpečnostné pravidlá pre fyzickú bezpečnosť, bezpečnosť prostredia a správu koncových zariadení prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:

42.	sú definované a používané bezpečnostné perimetre na ochranu oblastí, ktoré obsahujú aktíva používané v sieťach, informačných systémoch a operačných technológiách
43.	priestory, v ktorých sa nachádzajú riadiace a serverové súčasti informačných a operačných technológií, majú definované pravidlá fyzickej bezpečnosti
44.	fyzický prístup k vybraným aktívam infraštruktúry, ktoré sú klasifikované ako kritické alebo významné z hľadiska bezpečnosti a prevádzky, je povolený výhradne autorizovaným osobám
45.	je navrhnutá a zavedená fyzická bezpečnosť kancelárií, miestností a zariadení
46.	zabezpečené priestory sú nepretržite monitorované z hľadiska neoprávneného fyzického prístupu
47.	sú monitorované všetky prístupy do zabezpečených priestorov a je zabezpečená dohľadateľnosť pohybu
48.	aktíva v zabezpečených priestoroch sú chránené pred poškodením a neoprávneným zásahom zo strany zamestnancov pracujúcich v týchto priestoroch a nepovolaných osôb
49..	sú definované a primerane presadzované pravidlá čistého stola pre listinné dokumenty a prenosné pamäťové médiá a pravidlá pre čisté obrazovky zariadení na spracovanie informácií
50.	sa prijímajú opatrenia na zabránenie strate, poškodeniu, krádeži alebo kompromitácii zariadení používaných, prenášaných a uchovávaných mimo pracoviska a sú definované postupy, ak k takejto udalosti dôjde
51.	pamäťové médiá sú riadené počas ich životného cyklu, t. j. počas ich získavania, používania, prepravy a likvidácie, v súlade s klasifikačnou schémou a požiadavkami na manipuláciu s nimi
52.	dáta uložené v koncových zariadeniach používateľov, spracúvané týmito zariadeniami alebo prístupné prostredníctvom nich, sú chránené
53.	informácie uložené v informačných systémoch, zariadeniach alebo na iných pamäťových médiách sú vymazané, ak už nie sú potrebné
	Bezpečnostné pravidlá pre ochranu záznamov, súkromia a označovanie informácií prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
54.	informácie sú klasifikované na základe potrieb prevádzkovateľa základnej služby a na základe požiadaviek na dôvernosť, integritu, dostupnosť a špecifických požiadaviek zainteresovaných strán
55.	záznamy sú primerane chránené pred stratou, zničením, falšovaním, neoprávneným prístupom a neoprávneným zverejnením
56.	je zabezpečené plnenie požiadaviek týkajúcich sa ochrany osobných údajov podľa osobitných predpisov a zmluvných požiadaviek

	Bezpečnostné pravidlá pre dodávateľský reťazec prijíma výskumný subjekt, ktorý nie je prevádzkovateľom základnej služby tak, že:
57.	sú definované a zavedené procesy a postupy na riadenie kybernetických rizík spojených s používaním produktov, procesov alebo služieb tretích strán

Príloha č. 2
k vyhláške č. .../2026 Z. z.

OPATRENIA
NA OCHRANU KYBERNETICKEJ BEZPEČNOSTI A INFORMAČNEJ BEZPEČNOSTI PRI SPRÍSTUPNENÍ DÔVERNÝCH ŠTATISTICKÝCH ÚDAJOV NA VEDECKÝ ÚČEL PROSTREDNÍCTVOM SYSTÉMU VZDIALENÉHO PRÍSTUPU K DÔVERNÝM ŠTATISTICKÝM ÚDAJOM