Národní úřad
pro kybernetickou
a informační bezpečnost

NÚKIB

Brno 24. září 2025

Č. j. 7744/2025-NÚKIB-E/210

NUKIX004V21W

Věc: Poskytnutí informací podle § 14 odst. 5 písm. d) zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů

Vážený pane [redacted]

Národní úřad pro kybernetickou a informační bezpečnost (dále jen jako „**Úřad**“) obdržel dne 1. září 2025 Vaši žádost podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů. V žádosti požadujete poskytnutí informací týkajících se Koncepce ochrany neutajovaných informací citlivé povahy. Tímto Vám sděluji, ve struktuře dle Vaší žádosti, následující informace:

„Chtěl bych touto cestou požádat ve smyslu zákona o svobodném přístupu k informacím o poskytnutí Koncepce ochrany neutajovaných informací citlivé povahy, a výčet jednotlivých kroků koncepce, které již byly realizovány.“

Odpověď: Koncepce ochrany neutajovaných informací citlivé povahy je přílohou této odpovědi. Ve druhé části dotazu Úřad uvádí, že mu není známo, že by byly některé kroky doposud realizovány a doporučuje žadateli obrátit se na Ministerstvo vnitra České republiky jako na gestora odpovědného za zpracování tohoto úkolu.

S pozdravem

[redacted]

Mgr. Vít Hrazdíra
vedoucí oddělení právního
Národní úřad pro kybernetickou
a informační bezpečnost

Obdrží:
[redacted]

Vypraveno dne:
viz časový údaj na obálce datové zprávy

NÚKIB

Národní úřad
pro kybernetickou
a informační
bezpečnost

KONCEPCE OCHRANY NEUTAJOVANÝCH INFORMACÍ CITLIVÉ POVAHY

Obsah

1 Manažerské shrnutí

- Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) předkládá Koncepci ochrany neutajovaných informací citlivé povahy (dále jen „Koncepce“), jejímž cílem je analýza nedostatků současného stavu v oblasti nakládání a sdílení neutajovaných informací, stanovení vize cílového stavu a koncepční návrh variant řešení.
- Objektem Koncepce jsou neutajované informace citlivé povahy (dále jen „citlivé neutajované informace“), tedy informace, kterým je vlastní vysoká míra důležitosti a citlivosti, avšak nespadají do informací utajovaných podle zákona č. 412/2005, o ochraně utajovaných informací a o bezpečnostní způsobilosti.
- Zpracování Koncepce vychází z úkolu č. 83 Akčního plánu k Národní strategii kybernetické bezpečnosti pro období let 2021 až 2025. NÚKIB byl úkol přidělen jakožto gestorovi kybernetické bezpečnosti, neboť citlivé neutajované informace citlivé jsou v rámci státní správy často zpracovávány právě v informačních systémech.
- Aktuálně v České republice (dále jen „ČR“) neexistuje závazná definice citlivých neutajovaných informací. Právní řád ČR definuje a výslovně reguluje pouze dílčí kategorie citlivých neutajovaných informací (např. osobní údaje, EU LIMITE nebo zvláštní skutečnosti).
- Státní instituce využívají své vlastní, interně zavedené a vzájemně nekompatibilní systémy klasifikace a označování neutajovaných informací, což ztěžuje sdílení informací mezi relevantními státními orgány. Nejednotnost klasifikace a označování citlivých neutajovaných informací zároveň komplikuje zavedení zautomatizovaných postupů a vytvoření jednotných zabezpečených systémů pro jejich sdílení napříč státní správou. Nejcitlivější kategorie neutajovaných informací není dostatečně chráněna před neoprávněným přístupem.
- Jednotlivé stávající systémy ochrany citlivých neutajovaných informací jsou nevyhovující, jelikož neodpovídají potřebám moderní a efektivní státní správy, komplikují sdílení informací napříč jednotlivými institucemi či subjekty a zvyšují riziko nežádoucího poskytnutí informací mimo určený okruh adresátů.
- S ohledem na identifikované nedostatky je vizí Koncepce vytvoření a zavedení efektivního a uživatelsky přívětivého modelu klasifikace, označování a ochrany citlivých neutajovaných informací a nakládání s nimi, který bude široce využívaný a bude odpovídat soudobým požadavkům státní správy, zejména co se týče zpracování informací v informačních a komunikačních systémech.
- K naplnění vize navrhuje Koncepce pět strategických cílů a čtyři alternativní varianty řešení, lišící se komplexností a mírou potřeby legislativních změn:
    - Varianta A navrhuje vytvoření obecně závazného jednotného systému klasifikace, označování a ochrany neutajovaných informací. Tato varianta obnáší změnu právního řádu.

- Varianta B nepředpokládá legislativní změny a navrhuje vytvoření jednotného systému klasifikace, označování a ochrany neutajovaných informací v rozsahu možném bez legislativní změny. Systém by byl prostřednictvím usnesení vlády závazný pouze pro ústřední orgány státní správy. Pro ostatní subjekty, včetně soukromoprávních, by byl využitelný dobrovolně.
- Varianta C kombinuje obě předchozí varianty a navrhuje přednostní realizaci varianty B (vytvoření a postupné zavádění systému nevyžadujícího legislativní změny) společně se zahájením prací na postupné implementaci varianty A (vytvoření závazného systému prostřednictvím legislativní změny).
- Nulová varianta předpokládá ponechání současného stavu.

- **Navrhuje se, aby Bezpečnostní rada státu vybrala variantu řešení A a pověřila Ministerstvo vnitra (dále jen „MV“) ve spolupráci s Ministerstvem obrany (dále jen „MO“) a NÚKIB jejím rozpracováním do podoby konkrétního návrhu řešení, a to do 31. prosince 2027.**

2 Úvod

Koncepce si klade za cíl nastavit národní vizi a strategické směřování v ochraně a sdílení citlivých neutajovaných informací. Koncepce vychází z *Národní strategie kybernetické bezpečnosti ČR 2021-2025*, konkrétně z úkolu č. 83 *Akčního plánu k Národní strategii kybernetické bezpečnosti pro období let 2021 až 2025.* Její podoba pak reflektuje *Metodiku přípravy veřejných strategií.*

Koncepce vznikla pod koordinací NÚKIB, přičemž se na jejím zpracováním podíleli zástupci Bezpečnostní informační služby (dále jen „BIS"), MO, MV, Ministerstva zahraničních věcí (dále jen „MZV"), Národního bezpečnostního úřadu (dále jen „NBÚ"), Úřadu pro zahraniční styky a informace (dále jen „ÚZSI") a Vojenského zpravodajství (dále jen „VZ").

BOX 1: Základní pojmy

Data
= záznamy jednání, skutečností nebo informací a soubory takových jednání, skutečností nebo informací, včetně provozních údajů a metadat, zejména v podobě textu, čísel, grafů, obrazů, zvuku a videa.

Informace
= zpracovaná, interpretovaná nebo uspořádaná data, která mají význam a kontext.

Nosiče dat (datová média)
= Různé formy či metody, pomocí kterých lze data/informace ukládat, přenášet nebo zobrazovat.
= Nejpoužívanějšími nosiči dat jsou: papír, magnetické disky (např. pevný disk v počítači), optické disky (CD, DVD, Blue-Ray), optické vlákno, mikrofilm, flash paměti (USB, SD karty a další polovodičové disky), magnetické pásky, cloudová úložiště a zvukové nebo rádiové vlny.

Informační bezpečnost = Ochrana informací ve všech jejich formách (digitální i fyzické) po celý jejich životní cyklus.

Kybernetická bezpečnost = Souhrn právních, organizačních, technických a vzdělávacích prostředků směřujících k zajištění ochrany kybernetického prostoru, včetně informací v kyberprostoru vzniklých nebo v něm zpracovávaných.

3 Analýza současného stavu a definice problému

Za citlivé neutajované informace lze obecně označit takové informace, které jsou citlivé, avšak nespadají do informací utajovaných. Stávající systém ochrany tohoto typu informací je nedostačující. Jak je detailněji popsáno níže v podkapitolách 3.2 až 3.7, současný přístup státní správy k citlivým neutajovaným informacím se potýká s chybějící jednotnou definicí, rozdílnou klasifikací, roztříštěným označováním a v důsledku i s nedostatečnou ochranou. Aktuální stav neodpovídá potřebám moderní a efektivní státní správy, komplikuje sdílení informací mezi jednotlivými státními orgány a zvyšuje riziko nežádoucího poskytnutí informací mimo určený okruh adresátů.

3.1 Hlavní aktéři státní správy v oblasti ochrany informací

Hlavními aktéry státní správy v oblasti ochrany informací jsou BIS, Digitální informační agentura (dále jen „DIA"), MO, MV, NBÚ, NÚKIB, Úřad pro ochranu osobních údajů (dále také „ÚOOÚ"), ÚZSI a VZ.

MO je ústředním orgánem státní správy pro zabezpečování obrany státu.

MV je ústředním orgánem státní správy pro vnitřní záležitosti. Kromě vnitřního pořádku a bezpečnosti spadá do jeho gesce mj. také spisová služba, péče o archiválie, matriky a evidence obyvatel. Část pravomocí a aktivit MV v oblasti eGovermentu, digitalizace a informačních systémů veřejné správy byla k 1. lednu 2023 převedena na nově vzniklou DIA. MV je také gestorem zákona o archivnictví a spisové službě.[1] Dále je MV gestorem oblasti svobodného přístupu k informacím z veřejné správy.

NBÚ je ústředním správním orgánem v oblasti ochrany utajovaných informací a bezpečnostní způsobilosti. Vydává osvědčení a doklady o bezpečnostní způsobilosti a dále povoluje poskytování utajovaných informací v rámci mezinárodního styku. Jeho činnost je primárně dána zákonem o ochraně utajovaných informací.[2]

NÚKIB je ústředním správním orgánem pro kybernetickou bezpečnost a pro ochranu utajovaných informací v oblasti informačních a komunikačních systémů a kryptografické ochrany. Dále má na starosti agendu veřejně regulované služby v rámci družicového systému Galileo. Vznikl 1. srpna 2017 na základě novely[3] zákona o kybernetické bezpečnost[4] (dále jen ZKB“), jehož je také gestorem.

DIA byla zřízena v lednu 2023 novelou zákona o právu na digitální služby[5] jako ústřední správní úřad pro informační systémy veřejné správy, elektronickou identifikaci a služby vytvářející důvěru. DIA taktéž koordinuje oblasti centrálního řízení digitalizace a eGovernmentu. V případě přijetí návrhu zákona o správě dat a řízeném přístupu k datům,[6] bude DIA plnit roli jednotného informačního místa podle nařízení o evropské správě dat.[7] Podle návrhu novely zákona o základních registrech[8] by měla mít DIA do budoucna ve správě základní registr obyvatel a základní registr osob.

ÚOOÚ je ústředním dozorovým správním orgánem pro ochranu osobních údajů. Dále má mj. dílčí působnost nadřízeného, přezkumného a nečinnostního orgánu v oblasti práva na svobodný přístup k informacím.[9] Vznikl v roce 2000. Činnost úřadu vymezuje především GDPR[10] a zákon o zpracování osobních údajů.[11]

---

[1] Zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů (zákon o archivnictví)
Tento zákon upravuje spisovou službu včetně povinnosti identifikace a označování dokumentů v rámci činnosti veřejné správy a oblast archivnictví a péče o archiválie, které byly vybrány za archiválie zejména z dokumentů evidovaných ve spisových službách, samostatných evidencích dokumentů a v informačních systémech, které nejsou elektronickými systém spisové služby, které byly následně vybrány jako archiválie a vzaty do evidence Národního archivního dědictví.

[2] Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů (zákon o ochraně utajovaných informací).

[3] Zákon č. 205/2017 Sb., kterým se mění zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti).

[4] Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů.

[5] Zákon č. 12/2020 Sb., o právu na digitální služby a o změně některých zákonů.

[6] Stav materiálu k 1. 9. 2024: ukončeno mezirezortní připomínkové řízení; identifikační číslo v eKLEP: KORND4KLAAG6.

[7] Nařízení Evropského parlamentu a Rady (EU) 2022/868 ze dne 30. května 2022 o evropské správě dat a o změně nařízení (EU) 2018/1724 (akt o správě dat).

[8] Stav materiálu k 1. 9. 2024: zaevidováno v PSP; identifikační číslo v eKLEP: ALBSCU5BXBA0

[9] Zákon č. 106/1999 Sb., o svobodném přístupu k informacím (zákon o svobodném přístupu k informacím).

[10] Nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR).

[11] Zákon č. 110/2019 Sb., o zpracování osobních údajů (zákon o zpracování osobních údajů).

Zpravodajské služby: VZ je součástí Ministerstva obrany a provádí rozvědnou a kontrarozvědnou činnost se zaměřením na informace relevantní pro obranu státu.[12] **BIS** působí jakožto kontrarozvědná zpravodajská služba uvnitř území ČR.[13] **ÚZSI** se z pozice rozvědné zpravodajské služby zaměřuje na získávání a vyhodnocování zpravodajských informací, které mají původ v zahraničí. Působnost, postavení a koordinaci všech zpravodajských služeb ČR stanoví, mimo jiné, zákon o zpravodajských službách ČR.[14]

3.2 Chybějící obecná definice citlivých neutajovaných informací

Shrnutí: V ČR chybí jasná a v praxi použitelná obecná definice citlivých neutajovaných informací. Právní řád rozeznává pouze informace utajované a dále dílčí skupiny citlivých neutajovaných informací (např. osobní údaje, důvěrné informace podle zákoníku práce nebo zvláštní skutečnosti). Definice chybí i na čistě koncepční, tedy právně nezávazné úrovni.

Podle právního řádu ČR lze rozdělit informace na utajované a neutajované. Definici utajované informace obsahuje zákon o ochraně utajovaných informací a zní následovně: *„Informace v jakékoliv podobě zaznamenaná na jakémkoliv nosiči označená v souladu s tímto zákonem, jejíž vyzrazení nebo zneužití může způsobit újmu zájmu ČR nebo může být pro tento zájem nevýhodné, a která je uvedena v seznamu utajovaných informací.“* Zákon o ochraně utajovaných informací stanovuje, společně s dalšími relevantními právními předpisy[15], také pravidla ochrany utajovaných informací a sankcionuje jejich porušení.[16]

BOX 2: Citlivá neutajovaná informace – pracovní definice

= Neutajovaná informace zaznamenaná na jakémkoliv nosiči, která vyžaduje určitou míru důvěrnosti a ochrany, neboť její neoprávněné zveřejnění, použití, změna nebo zničení by mohlo způsobit újmu osobě, České republice nebo cizímu státu, kterého se informace týká.

Neutajovanými informacemi jsou veškeré informace, které nespadají do informací utajovaných. V rámci široké kategorie neutajovaných informací lze vyčlenit skupinu tzv. **citlivých neutajovaných informací (viz Box 2)**, kterým je vlastní vysoká míra důležitosti a citlivosti. Typicky se jedná o osobní údaje (např. rodné číslo či zdravotní stav), ekonomické údaje (např. údaje z kontrolních hlášení), obchodní tajemství a citlivé informace státní správy (např. interní strategické nebo bezpečnostní analýzy, které nesplňují zákonné náležitosti pro jejich utajení).

Právní řád ČR „citlivé neutajované informace“ jakožto obecnou kategorii nikterak nedefinuje, ani neupravuje. Rozlišuje pouze několik dílčích specifických skupin citlivých neutajovaných informací, např. osobní údaje (viz podkapitola 3.3). Obecné vymezení pojmu „citlivá neutajovaná informace“

[12] Zákon č. 289/2005 Sb., o Vojenském zpravodajství.
[13] Zákon č. č. 154/1994 Sb., o Bezpečnostní informační službě a zákon č. 153/1994 Sb., o zpravodajských službách České republiky.
[14] Zákon č. 153/1994 Sb., o zpravodajských službách České republiky.
[15] Např. zákon č. 40/2009 Sb., trestní zákoník ve znění pozdějších předpisů (trestní zákoník); vyhláška č. 363/2011 Sb., o personální bezpečnosti a o bezpečnostní způsobilosti, ve znění pozdějších předpisů; nebo vyhláška č. 275/2022 Sb., o administrativní bezpečnosti a o registrech utajovaných informací, vyhláška č. 528/2005 Sb., o fyzické bezpečnosti a certifikaci technických prostředků, ve znění pozdějších předpisů.
[16] Např. § 317 zákona č. 40/2009 Sb., trestního zákoníku, který stanoví trestný čin ohrožení utajované informace.

neexistuje ani na koncepční (nelegislativní) úrovni. Grafické schéma jednotlivých kategorií informací znázorňuje Obrázek 1 níže.

3.3 Kategorie jednotlivých typů citlivých neutajovaných informací

Shrnutí: Právní řád ČR definuje a výslovně reguluje pouze dílčí kategorie citlivých neutajovaných informací. Typicky to jsou osobní údaje, důvěrné informace podle zákoníku práce a zákona o veřejných zakázkách, dokumenty EU LIMITE a NATO UNCLASSIFIED, zvláštní skutečnosti podle krizového zákona a informace spadající pod výjimky z práva na svobodný přístup k informacím. Mimo tyto kategorie existuje velká množina citlivých neutajovaných informací, které specificky regulovány nejsou (citlivé interní resortní politiky, analýzy, neveřejná stanoviska a další).

Na úrovni zákona a unijní legislativy jsou definovány a regulovány pouze některé **kategorie citlivých neutajovaných informací**. Konkrétní pravidla pro identifikaci, evidenci, označování, držení a nakládání s těmito kategoriemi informacemi upravují, s různou mírou detailu, příslušné právní předpisy. Primárně se jedná o:

1) **Osobní údaje.** Ochrana osobních údajů se řídí úmluvou Rady Evropy č. 108,[17] GDPR, zákonem o zpracování osobních údajů (ZZOÚ)[18] a dalšími právní předpisy – například zákony regulující oblasti, které zpracovávají osobní údaje (např. zdravotnictví, zaměstnanecká data či bankovnictví).

2) **Důvěrné informace/údaje** (neutajované) např. podle zákoníku práce[19] nebo zákona o veřejných zakázkách.[20]

3) **Informace, u kterých se ČR na mezinárodní úrovni zavázala, že je neposkytne třetí straně bez souhlasu původce.**[21] Primárně se jedná o citlivé neutajované dokumenty poskytnuté ČR Severoatlantickou aliancí (dokumenty „NATO UNCLASSIFIED“) nebo orgány či institucemi Evropské unie (dokumenty „EU LIMITE“). Podrobnější popis systému ochrany neutajovaných

[17] Úmluva o ochraně osob se zřetelem na automatizované zpracování osobních dat, ETS No. 108, přijata dne 28. ledna 1981 ve Štrasburku, ratifikována ČR dne 9. července 2001.
[18] Zákon č. 110/2019 Sb., o zpracování osobních údajů.
[19] § 276 odst. 3 zákona č. 262/2006 Sb., zákoník práce (zákoník práce): Důvěrnou informací se rozumí informace, jejíž poskytnutí může ohrozit nebo poškodit činnost zaměstnavatele nebo porušit oprávněné zájmy zaměstnavatele nebo zaměstnanců.
[20] § 218 odst. 1 zákona č. 134/2016 Sb., zákona o veřejných zakázkách (zákon o veřejných zakázkách): Za důvěrné se považují údaje nebo sdělení, které dodavatel poskytl zadavateli v zadávacím řízení a označil je jako důvěrné.
§ 33 téhož zákona: „[…] zadavatel [je] oprávněn vést tržní konzultace s odborníky či dodavateli s cílem připravit zadávací podmínky a informovat dodavatele o svých záměrech a požadavcích, pokud to nenarušuje hospodářskou soutěž.“
§ 218 odst. 3 téhož zákona: „Zadavatel nemusí uveřejnit informaci podle tohoto zákona, pokud by její uveřejnění znamenalo porušení jiného právního předpisu nebo by bylo v rozporu s veřejným zájmem, nebo by mohlo porušit právo dodavatele na ochranu obchodního tajemství nebo by mohlo ovlivnit hospodářskou soutěž.“
[21] V právním řádu ČR je tato povinnost promítnuta do § 64a odst. 1 zákona o archivnictví: „Dokument poskytnutý Organizací Severoatlantické smlouvy nebo Evropskou unií je v zájmu bezpečnosti státu, veřejné bezpečnosti nebo ochrany práv třetích osob chráněn uvedenými původci označením "NATO UNCLASSIFIED" nebo "LIMITE". V ČR je toto označení respektováno z důvodů plnění povinností vyplývajících z jejího členství v Organizaci Severoatlantické smlouvy nebo Evropské unii; s takovým dokumentem se může seznamovat osoba, která jej nezbytně potřebuje k výkonu své funkce, k pracovní nebo jiné obdobné činnosti. Jiné osobě může být takový dokument poskytnut se souhlasem původce a za jím stanovených podmínek.

informací Evropské unie (dále jen „EU“) a Severoatlantické aliance (dále jen „NATO“) obsahuje Příloha 2.

4) **Dokumenty označené OMEZENÝ PŘÍSTUP** podle § 64b zákona o archivnictví a nařízení vlády č. 243/2024 Sb., o dokumentech v oblasti obrany s omezeným přístupem. Jedná se o dokumenty v oblasti obrany, které ČR poskytl členský stát NATO, EU nebo jiný stát, se kterým ČR spolupracuje při výměně informací v oblasti obrany.[22] Takto označený dokument je přístupný pouze osobě, která jej potřebuje k výkonu své funkce, k pracovní nebo jiné obdobné činnosti v oblasti obrany. Jiné osobě se poskytuje pouze se souhlasem státu původce a za jím stanovených podmínek.

5) **Zvláštní skutečnosti podle krizového zákona.**[23] Neutajované údaje z oblasti krizového řízení, které by v případě zneužití mohly vést ke znemožnění nebo omezení činnosti orgánu krizového řízení, ohrožení života a zdraví osob, majetku, životního prostředí nebo podnikatelského zájmu právnické osoby nebo fyzické osoby vykonávající podnikatelskou nebo jinou obdobnou činnost podle zvláštních právních předpisů. Nakládání s informacemi s označením „zvláštní skutečnosti“ upravuje krizový zákon.

6) **Dokumenty vznikající v agendě ochrany oznamovatelů podle zákona o ochraně oznamovatelů (tzv. whistleblowerů).**[24]

7) **Další dílčí kategorie informací**; například informace, které tvoří obchodní tajemství, informace podléhající mlčenlivosti či informace chráněné autorskými právy.

8) **Informace spadající pod výjimky z práva na svobodný přístup k informacím podle zákona o svobodném přístupu k informacím a dalších relevantních zákonů.**[25] Podle čl. 17 Listiny základních práv a svobod ČR má každý právo na svobodný přístup k informacím o sobě samém a přístup k informacím ve veřejném zájmu. Toto právo lze omezit pouze zákonem, jde-li zároveň o opatření v demokratické společnosti nezbytné pro ochranu práv a svobod druhých, bezpečnost státu, veřejnou bezpečnost, ochranu veřejného zdraví a mravnosti. Množina informací, které se na základě výjimky z práva na svobodný přístup k informacím neposkytují nebo poskytují pouze omezeně, se částečně překrývá s předchozími sedmi kategoriemi.

Mimo tyto dílčí kategorie citlivých neutajovaných informací existuje i množina citlivých neutajovaných informací, které zákonem specificky vymezené a upravené nejsou. Zpravidla se jedná o interní dokumenty s citlivým obsahem, které jsou sice neutajované, avšak stát má legitimní zájem na tom regulovat jejich šíření a dostupnost. Například tedy interní resortní politiky, analýzy, dílčí bezpečnostní analýzy, informace o fyzickém zabezpečení objektů, informace týkající se fungování bezpečnostních sborů, Armády České republiky a tajných služeb, zejména pak informace o technickém zabezpečení jednotek, prostředcích a jejich kvantitě, personálním zabezpečení, a různá neveřejná stanoviska či neveřejné strategické informace. **Tato kategorie je z pohledu ochrany informací nejvíce problematická, neboť**

[22] Zákon č. 197/2024, kterým se mění zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů, ve znění pozdějších předpisů, zákon č. 261/2021 Sb., kterým se mění některé zákony v souvislosti s další elektronizací postupů orgánů veřejné moci, ve znění pozdějších předpisů a zákon č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.

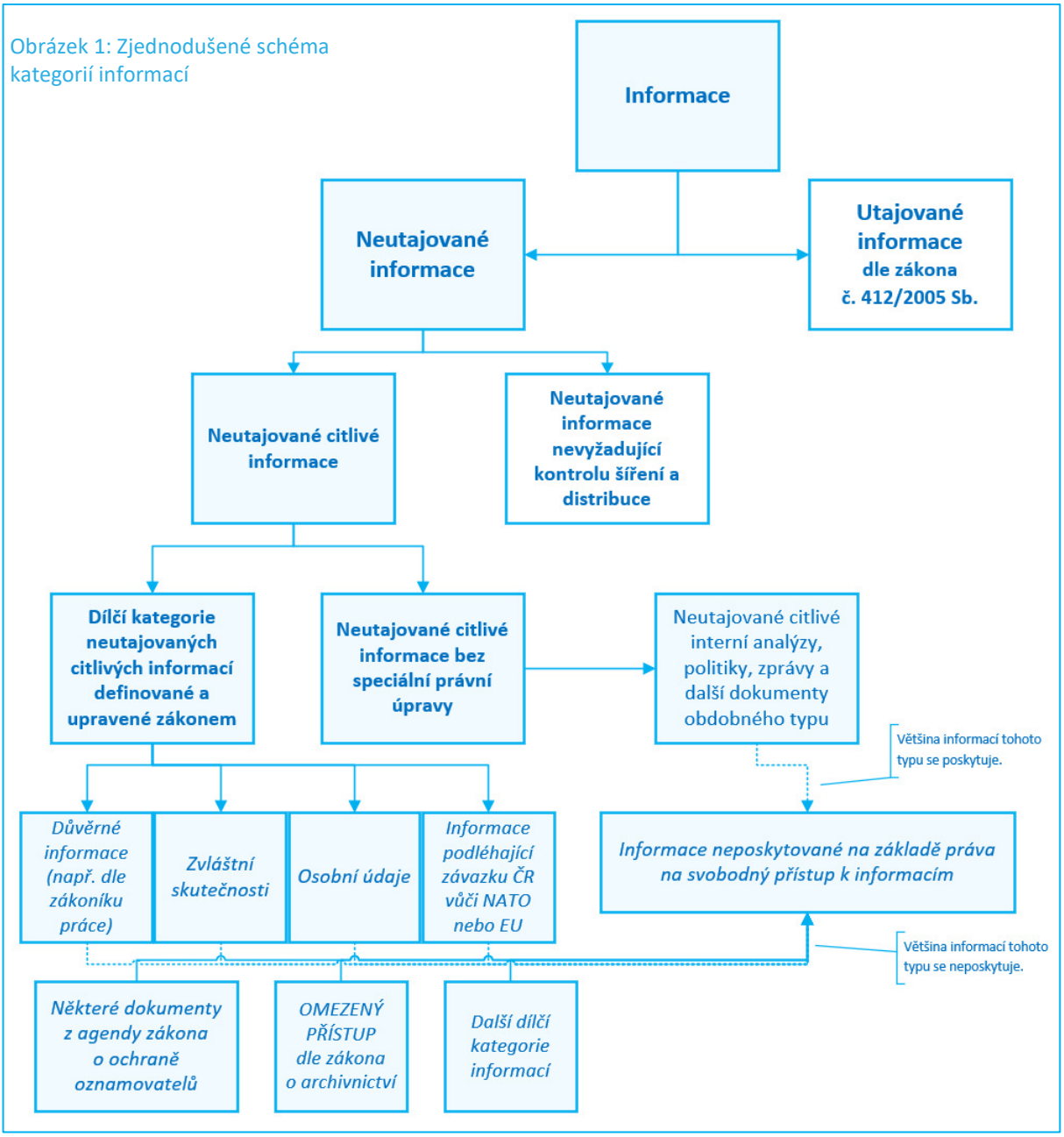
[23] § 27 odst. 1 zákona č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů, ve znění pozdějších předpisů (krizový zákon). V roce 2024 probíhají práce na novelizaci zákona o krizovém řízení – v rámci této novelizace se předpokládá zrušení kategorie informací „zvláštní skutečnosti podle krizového zákona“.

[24] Zákon č. 171/2023 Sb., o ochraně oznamovatelů.

[25] Například § 10a zákona o kybernetické bezpečnosti nebo § 8 a § 8a zákona o právu na informace o životním prostředí.

napříč státní správou aktuálně[26] chybí její jednotné vymezení, způsob označování a obecná pravidla pro sdílení.

Obrázek 1: Zjednodušené schéma kategorií informací



Zdroj: NÚKIB

[26] Obecná pravidla pro sdílení informací by měla být stanovena zákonem o správě dat o řízeném přístupu k datům. Stav návrhu zákona k 1. 9. 2024: ukončeno mezirezortní připomínkové řízení; identifikační číslo v eKLEP: KORND4KLAAG6.

3.4 Veřejné a neveřejné informace a jejich poskytování

Shrnutí: Veškeré neutajované informace, které státní správa vytváří a s kterými manipuluje, lze rozdělit na veřejné a neveřejné. Do veřejných informací spadají informace aktivně zveřejňované státní správou a informace poskytnuté na žádost v souladu s čl. 17 Listiny základních práv a svobod. Do neveřejných informací spadají informace, které se poskytují na žádost, ale ještě poskytnuty nebyly a informace, které se ani na žádost neposkytují. Citlivost informace určuje, po zohlednění relevantních právních a interních předpisů, její původce.

Jedním ze základních principů v oblasti ochrany informací je, že citlivost informace by měl (v souladu s platnými právními normami a interními předpisy) posoudit a stanovit její původce. Každý státní orgán má tudíž povinnost jakoukoliv informaci, kterou vytvořil nebo obdržel od třetí strany a upravil, posoudit a zajistit, aby byla chráněna v souladu s odpovídajícími zákonnými požadavky.

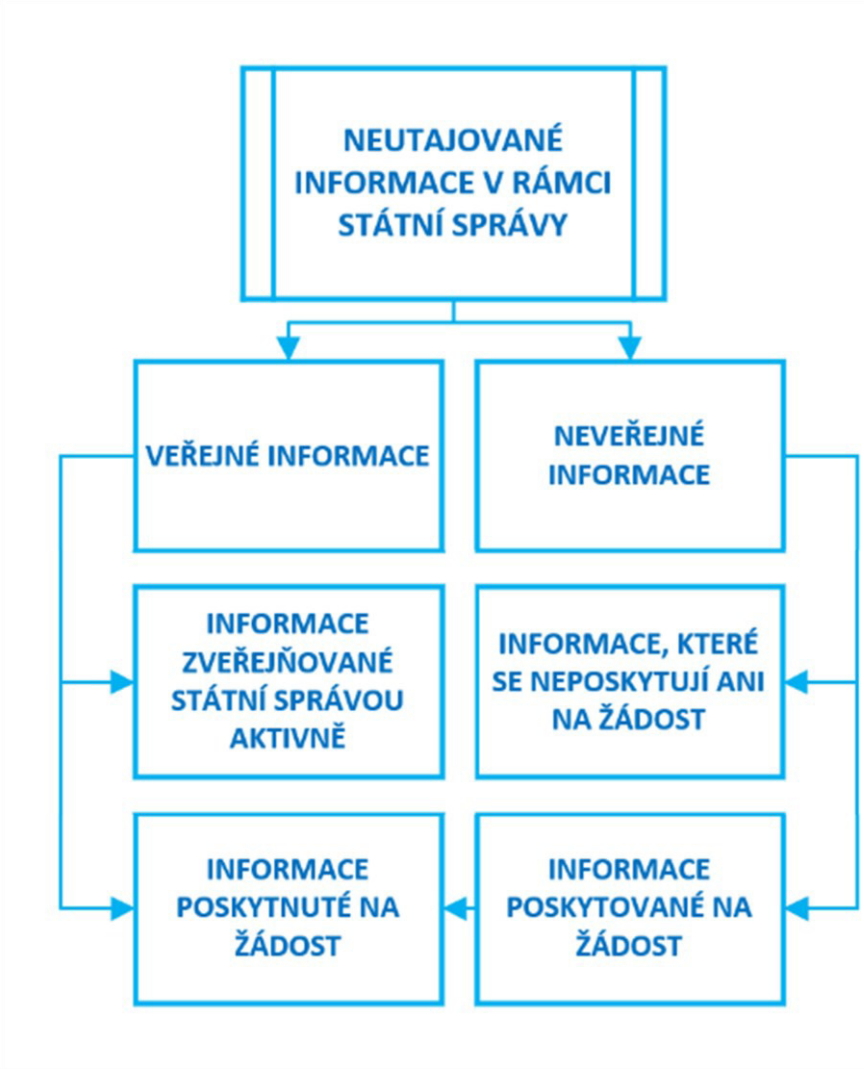
Každý státní orgán je zároveň zodpovědný za řádné posouzení toho, jaké informace je povinen zveřejňovat, popřípadě poskytovat. Na základě čl. 17 Listiny základních práv a svobod, který se promítá do zákona o svobodném přístupu k informacím a dalších relevantních zákonů[27], mají orgány státní správy povinnost fungovat transparentně a poskytovat informace vztahující se k jejich působnosti. V případě informací, které nejsou volně dostupné, mají fyzické a právnické osoby právo podat žádost o jejich poskytnutí. Typ a rozsah informací, které se poskytují, určuje zákon. Výjimky z poskytování informací stanoví primárně (ale nikoliv výlučně) zákon o svobodném přístupu k informacím a zákon o právu na informace o životním prostředí. Dílčí výjimky obsahují i některé další zákony, např. ZKB v § 10a.

Veškeré neutajované informace, které státní správa vytváří a s kterými nakládá, lze rozdělit na veřejné a neveřejné. Veřejné informace jsou takové, k nimž má přístup veřejnost, tj. okruh jejich příjemců je teoreticky neomezený. Do veřejných informací spadají informace aktivně poskytované státní správou a rovněž informace, které byly v souladu s čl. 17 Listiny základních práv a svobod a s ním souvisejících zákonů poskytnuty na vyžádání. Neveřejné informace jsou určeny limitovanému okruhu příjemců a spadají do nich informace, které se poskytují na žádost, ale ještě poskytnuty nebyly a informace, které se ani na vyžádání neposkytují. U kategorií citlivých neutajovaných informací, které zákon výslovně definuje a reguluje (např. osobní údaje), stanoví právní řád konkrétní pravidla zacházení s danými informacemi včetně toho, kdy a za jakých podmínek je možné je poskytnout třetím osobám. U informací, které do žádné z těchto definovaných kategorií nespadají a zároveň se poskytují na vyžádání, obecná pravidla platná pro celou státní správu stanovena nejsou.

V tomto kontextu je důležité připomenout, že obecná množina neveřejných informací je větší než množina neveřejných informací, které se ani na žádost neposkytují. Existují informace, které stát na základě legitimních důvodů preferuje nezveřejňovat, tedy aktivně nepodporovat jejich šíření v rámci veřejnosti, avšak v případě, že by o tyto nezveřejněné informace bylo v souladu se zákonem o svobodném přístupu k informacím požádáno a nespadaly pod některou ze zákonných výjimek, měl by dožádaný orgán povinnost je poskytnout. Analogicky tak i v rámci obecné kategorie neutajovaných informací existuje množina informací, které – ač je orgány veřejné správy preferují proaktivně nezveřejňovat – musí být v případě řádně podané žádosti poskytnuty.

[27] Např. zákon č. 123/1998 Sb., o právu na informace o životním prostředí (zákon o právu na informace o životním prostředí).

Obrázek 2: Informace podle míry veřejnosti a poskytování



Zdroj: NÚKIB

3.5 Vliv právní úpravy cílící na ochranu informací v kyberprostoru

Shrnutí: Kybernetickou a informační bezpečnost v ČR významným způsobem ovlivnilo přijetí zákona o kybernetické bezpečnost a navazujících prováděcích předpisů. Regulované subjekty jsou povinny mít přehled o informacích, které zpracovávají jejich informační a komunikační systémy, ohodnotit důvěrnost těchto informací a přijmout opatření k jejich ochraně.

Povinnosti a opatření podle zákona o kybernetické bezpečnosti a navazujících prováděcích předpisů nemohou samy o sobě nahradit jednotný systém ochrany, klasifikace, označování a sdílení citlivých neutajovaných informací, ale mohou představovat vhodnou výchozí pozici pro jeho vytvoření.

V dnešním globalizovaném světě představuje kyberprostor (viz Box 3)[28] klíčovou platformu pro přenos informací, což z něj činní neodmyslitelnou součást fungování (nejen) státních institucí. Rozvoj informačních technologií zároveň vede k postupnému stírání hranic mezi fyzickým a digitálním světem, zvyšování závislosti moderní společnosti na informačních a komunikačních technologiích a nárůstů rizik spojených s využíváním kyberprostoru. S tímto vývojem nabývá na důležitosti i otázka ochrany bezpečnosti informací v kyberprostoru (viz Box 4).[29]

BOX 3: Kyberprostor

Kyberprostor je digitální prostředí umožňující vznik, zpracování a výměnu informací, tvořené informačními systémy a službami a sítěmi elektronických komunikací.

Ochranu bezpečnosti informací v kyberprostoru řeší primárně dva zákony – ZKB a zákon o ochraně utajovaných informací. Vzhledem k zaměření této Koncepce pouze na citlivé neutajované informace, se následující text věnuje pouze ZKB. To však nevylučuje skutečnost, že označování a ochranu citlivých neutajovaných informací je nutné řešit i v prostředí klasifikovaných informačních systémů. Zároveň je nutné zohlednit označování a manipulaci s dokumenty obsahujícími citlivé neutajované informace i v elektronických systémech spisové služby.

BOX 4: Bezpečnost informace podle § 2 písm. c) zákona o kybernetické bezpečnosti

Zajištění důvěrnosti, integrity a dostupnosti informace v průběhu celého jejího životního cyklu.

ZKB a vyhláška o kybernetické bezpečnosti (dále jen „VKB“)[30] požadují od povinných osob zavedení tzv. systému řízení bezpečnosti informací (dále jen „ISMS“, zkratka z anglického *„Information Security Management System“*)[31] a přijetí opatření k zajištění bezpečnosti informací vzniklých či zpracovávaných v kybernetickém prostoru. V rámci bezpečnostních opatření podle ZKB mají regulované osoby povinnost vykonávat tzv. řízení aktiv a rizik[32]. Jedním z typů aktiv jsou informace, které zpracovávají nebo poskytují informační a komunikační systémy (viz Box 5). Nejčastěji se jedná o informace zpracovávané a vytvářené při výkonu agendy nebo v rámci informačních systémů (včetně logů a metadat),

[28] Definice podle stávající platné legislativy. Připravovaný nový zákon o kybernetické bezpečnosti definuje v § 2 odst. 2 písm. a) kyberprostor mírně odlišně: „Soubor sítí elektronických komunikací a dalších technologií, ve kterém dochází ke zpracování informací a dat v elektronické podobě“

[29] Definice podle stávající platné legislativy. Připravovaný nový zákon o kybernetické bezpečnosti definuje bezpečnost informací mírně odlišně: „Zajištění důvěrnosti, integrity a dostupnosti informací a dat.“

[30] Vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat.

[31] ISMS se rozumí ta část systému řízení organizace založená na přístupu k rizikům informačního nebo komunikačního systému, která stanoví způsob ustavení, zavádění, provozování, monitorování, přezkoumání, udržování a zlepšování bezpečnosti informací a dat.

[32] § 5 odst. 2 zákona o kybernetické bezpečnosti.

vlastní data agendy, záznamy o provozu, data o uživatelích, přístupové údaje, data relací, konfigurační soubory, zdrojové kódy, zálohy a certifikáty.

Všude tam, kde je to relevantní, musí být do analýzy zahrnut i fyzický svět. Kybernetická bezpečnost tak v mnoha případech zahrnuje i fyzickou bezpečnost. Například datacentrum, ve kterém jsou ukládány informace, musí být fyzicky chráněno tak, aby se do něj nedostala nepovolaná osoba, u nosičů informací musí být zajištěna odolnost vůči různým klimatickým vlivům a důvěrnost vytištěných dokumentů je nutné chránit na stejné úrovni jako důvěrnost jejich elektronických originálů.[33]

BOX 5: Aktiva podle ZKB

Kybernetické bezpečnostní prvky, které je regulovaný subjekt povinen chránit.

Podle VKB se aktiva dělí na primární (informace nebo služba, kterou zpracovává nebo poskytuje informační a komunikační systém) a podpůrná (technické vybavení, komunikační prostředky a programové vybavení informačního systému, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačních systémů).

Součástí řízení aktiv (viz Obrázek 3 níže) je také proces jejich identifikace a hodnocení.[34] Cílem procesu hodnocení aktiv je určit, jaký má dané aktivum pro povinný subjekt význam a jak velký dopad by mělo jeho narušení na běžný chod daného subjektu (např. státního úřadu). Aspekty aktiv, které by měly být hodnoceny, shrnuje tzv. CIA triáda, tedy, C – Confidentiality (důvěrnost), I – Integrity (integrita) a A – Availability (dostupnost).

Důvěrnost v tomto kontextu znamená, pro jaký okruh osob je dané aktivum přístupné (viz Box 6). VKB doporučuje regulovaným osobám hodnotit důvěrnost informací na čtyřstupňové škále – nízká, střední, vysoká a kritická (viz Příloha 4). Po identifikovaní a ohodnocení aktiv jsou regulované osoby povinny přijmout přiměřená bezpečností opatření k zajištění adekvátní úrovně bezpečnosti informací. Přijatá opatření musí brát v potaz celý životní cyklus služeb a informací, a také možná propojení s jinými organizacemi nebo systémy. Mezi regulované subjekty podle ZKB spadají všechny orgány státní správy.[35] **Všechny orgány státní správy jsou tak povinny mít přehled o informacích, které jsou součástí jejich ISMS a v rámci procesu hodnocení aktiv ohodnotit stupeň jejich důvěrnosti. Zároveň musí zavést přiměřená opatření k zajištění bezpečnosti těchto informací, tedy k zachování jejich důvěrnosti, integrity a dostupnosti.**[36]

BOX 6: Důvěrnost informace v kontextu kybernetické bezpečnosti

Důvěrnost informací perspektivou kybernetické bezpečnosti a ochrany dat se zaměřuje na ochranu citlivých a důvěrných informací před neoprávněným přístupem, zneužitím, ztrátou nebo odcizením v kyberprostoru.

Pro zachování důvěrnosti je nutné chránit informaci proti přístupu, který není autorizovaný.

Z pohledu ochrany a sdílení citlivých neutajovaných informací mají bezpečnostní záruky podle ZKB a VKB své limity, neboť tyto právní normy nebyly vytvořeny s cílem vytvořit jednotný systém ochrany a sdílení citlivých neutajovaných informací. Jejich prioritou je zajištění kybernetické a informační bezpečnosti. ZKB a VKB neupravují bezpečnost veškerých informací, se kterými povinné subjekty manipulují nebo které mají v držení. Vztahují se primárně na zabezpečení informací v kontextu kyberprostoru. Zde je nutné zdůraznit, že jasné vytyčení hranice mezi bezpečností informace

[33] Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti.pdf (nukib.cz))

[34] Blíže k identifikaci a řízení aktiv zde: Průvodce řízením aktiv a rizik dle vyhlášky o kybernetické bezpečnosti.pdf (nukib.cz)

[35] Speciální postavení mají obce s rozšířenou působností, na tyto ZKB zatím nedopadá. To by se mělo změnit s přijetím nového zákona o kybernetické bezpečnosti v roce 2024. Podle § 33 platného ZKB mají specifické postavení také zpravodajské služby, Generální inspekce bezpečnostních sborů a Policie ČR.

[36] Viz vyhláška o kybernetické bezpečnosti – část II.

v kyberprostoru a ve fyzickém světě je v praxi problematické, neboť kybernetická bezpečnost má přesah i do bezpečnosti fyzické (např. výše zmíněné zabezpečení datových center nebo bezpečnostní dokumentace v digitální či listinné podobě). Částečné upřesnění by měl přinést nově navrhovaný zákon o kybernetické bezpečnosti a na něj navazující vyhlášky, podle kterých se budou pravidla pro ochranu aktiv výslovně vztahovat i na listinné dokumenty, vyměnitelná zařízení a datové nosiče, které jsou kopií originálů v elektronické verzi.[37] **Chráněny tak budou muset být nejen elektronické verze dokumentů, ale i jejich fyzická forma.** Cílem je zamezit situacím, kdy by informace přestala být chráněna pouze proto, že byla přenesena do fyzické podoby – např. vytištěna na papír. Stále však bude existovat velmi úzká množina informací, na které se tato ochrana vztahovat nebude. Primárně se bude jednat informace zachycené pouze ve fyzické podobě bez jakéhokoliv elektronického zpracování nebo elektronické verze a bez vazby na kybernetickou bezpečnost.[38] Lze nicméně předpokládat, že v rámci státní správy se bude jednat o velmi malou množinu.

Dalším limitem z pohledu ochrany citlivých neutajovaných informací je skutečnost, že byť jsou podle ZKB regulované subjekty povinny v rámci ohodnocení aktiv posoudit každou informaci, která je součástí jejich ISMS, toto nezbytně neznamená ohodnocení každého dokumentu či informace individuálně. Častou a praktickou volbou na straně regulovaných subjektů je vytváření tzv. typových aktiv, tedy specifických skupin aktiv, které mají společné vlastnosti.[39] V praxi tak povinné subjekty zpravidla ohodnocují určitý typ dokumentu se standardizovaným obsahem (např. výplatní pásky všech zaměstnanců, lékařské záznamy o pacientech obsahující osobní údaje nebo standardní zákaznické smlouvy) stejnou hodnotou – bez individuálního posouzení každého jednotlivého dokumentu. Z pohledu ZKB a VKB je tento postup při dodržení výše uvedených podmínek dostačující, ovšem z pohledu identifikace a ochrany citlivých neutajovaných informací nikoliv. **ZKB a VKB například nevyžadují, aby povinné subjekty opatřily každou jednotlivou informaci označením úrovně důvěrnosti. Pro ochranu citlivých neutajovaných informací je naopak jednotné a přehledné označování každé informace klíčové**. Právě nejednotnost či přímo absence označení je jednou z hlavních překážek bránících efektivnímu sdílení citlivých neutajovaných informací napříč státní správou (viz podkapitola 3.6).

ZKB a VKB zároveň regulovaným osobám nepředepisují jeden konkrétní systém hodnocení aktiv. Povinné subjekty tak mohou volit různé způsoby hodnocení důvěrnosti informací za podmínky, že jejich postup naplňuje zákonem stanovené požadavky. Přístup v rámci státní správy je proto v praxi nejednotný a různé orgány používají pro hodnocení důvěrnosti informací odlišné, vzájemně nekompatibilní, metody a stupnice**. U některých orgánů státní správy také dochází ke dvojkolejnosti, kdy daná instituce používá jeden systém klasifikace a označování informací pro účely kybernetické bezpečnosti (např. TLP protokol) a jiný systém pro účely ochrany důvěrnosti citlivých informací (např. dělení informací na interní a pro veřejnost).** Perspektivou ZKB a VKB je tento přístup zcela v pořádku, nicméně koncepčně situaci komplikuje.

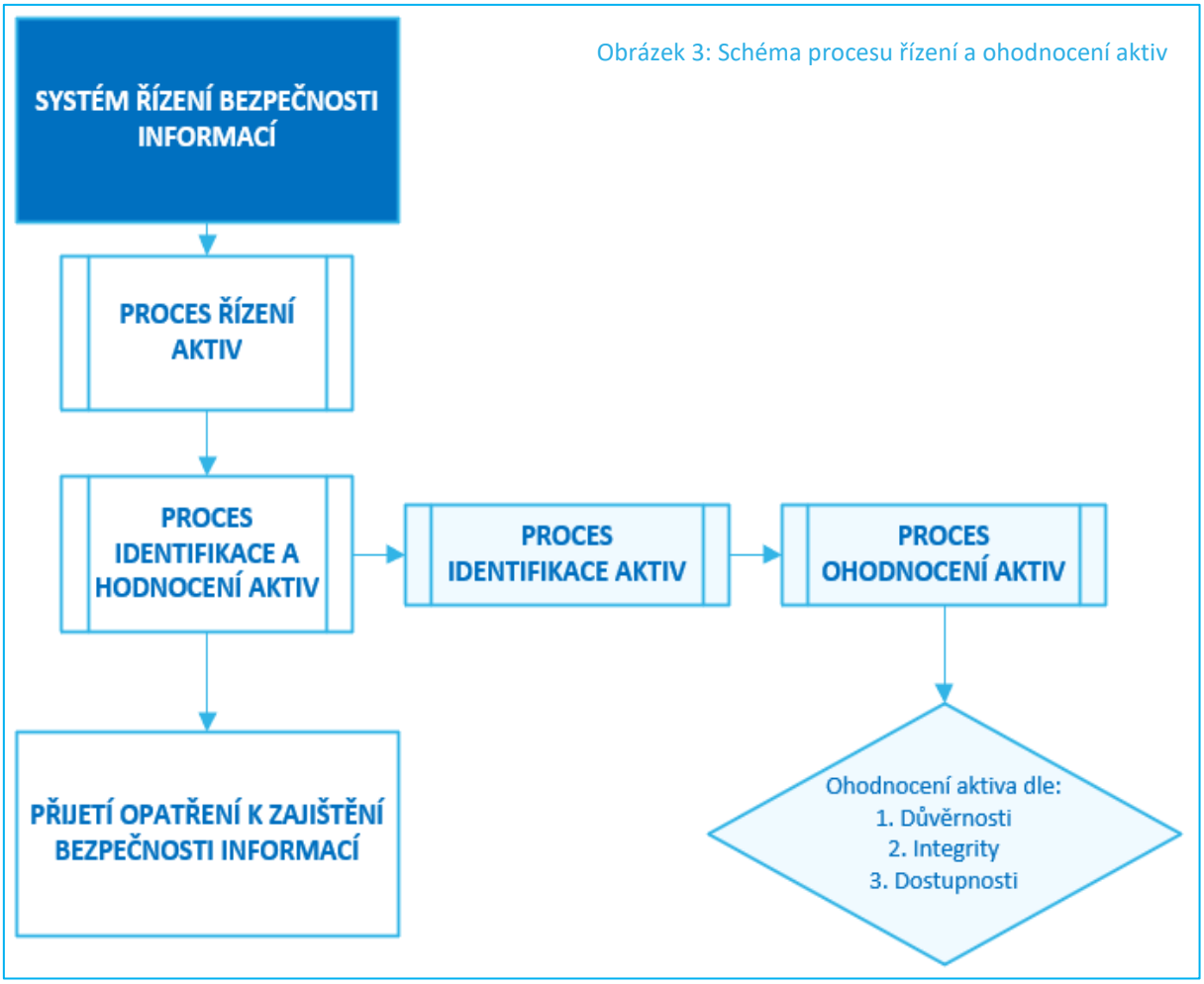
[37] Viz Příloha 4 návrhu vyhlášky o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností.

[38] Pro ilustraci lze uvést velmi nepravděpodobný scénář bezpečnostní dokumentace ISMS, která by byla dostupná pouze v listinné podobě, nikoliv v digitální. Vzhledem k tomu, že bezpečností dokumentace ISMS má zásadní vazbu na kybernetickou bezpečnost, vztahovala by se ochrana podle ZKB i na takovéto aktivum – přestože není v digitální podobě, ani nemá svůj digitální otisk.

[39] Seskupování aktiv musí být podloženo logickou úvahou a jednotlivá aktiva seskupená do jednoho typového aktiva si musí být svou povahou natolik podobná, aby na ně působily stejné hrozby a zranitelnosti. Zároveň se nesmí seskupovat aktiva, jejichž hodnocení se z pohledu důvěrnosti, integrity a dostupnosti významně liší.

Povinnosti vyplývající regulovaným subjektům ze ZKB a VKB (identifikace a ohodnocení aktiv včetně úrovně důvěrnosti) tak mohou již ve stávající podobě posloužit jako základní stavební blok pro jeho vybudování, ale samy o sobě plnohodnotně systém ochrany citlivých neutajovaných informací nenahradí.

Obrázek 3: Schéma procesu řízení a ohodnocení aktiv



Zdroj: NÚKIB

3.6 Klasifikace, označování a sdílení citlivých neutajovaných informací

Shrnutí: Aktuálně v rámci státní správy ČR neexistuje jednotný systém označování úrovně důvěrnosti neutajovaných informací, a to ani na právní, ani na koncepční úrovni. Pro některé dílčí kategorie informací (např. zvláštní skutečnosti nebo NATO UNCLASSIFIED) vyplývá tato povinnost ze zákona, není tomu však pro všechny kategorie neutajovaných informací.

Praxe napříč státní správou je roztříštěná. Resorty a instituce používají své vlastní systémy označování, které zpravidla zavádí prostřednictvím interních předpisů. Tyto systémy jsou často navzájem nekompatibilní. Obvyklým problémem je také nedostatečná důslednost, kdy některé z vytvořených informací nejsou jejich původci vůbec označeny. Nejednotnost klasifikace a označování výrazně komplikuje sdílení informací napříč státní správou i směrem k externím subjektům.

Kvalitní a funkční systém klasifikace a označování informací (viz Box 7) je jasný, konzistentní, relevantní vzhledem k povaze informací a snadno interpretovatelný, což zajišťuje správné třídění i ochranu dat. Pro ochranu citlivých neutajovaných informací je existence jednotného, efektivního a srozumitelného

systému klasifikace a označování klíčovým předpokladem. Takto fungující systém umožňuje rychlou identifikaci a správné zacházení s citlivými údaji, minimalizuje možnost neúmyslného úniku, podporuje budování důvěry mezi spolupracujícími složkami a orgány a napomáhá zajištění ochrany soukromí a bezpečnosti informací v rámci výkonu státní správy.

3.6.1 Označování informací ve státní správě

Pravidla pro označování dokumentů pramení ze dvou hlavních zdrojů – relevantních právních norem (např. krizový zákon nebo zákon o archivnictví a spisové službě) a interních aktů řízení daného úřadu či instituce (např. pokyn ministra)[40].

Identifikaci, označování, evidenci a správu neutajovaných dokumentů ve veřejné správě upravuje primárně zákon o archivnictví a spisové službě, který zavádí pravidla spisové služby a archivnictví v obecné rovině. Významně by měl tuto oblast ovlivnit také plánovaný zákon o správě dat a o řízeném přístupu k datům, který je nyní v legislativním procesu.[41]

BOX 7: Označování (labeling) informací

Označování v oblasti správy informací znamená systematické označování dat nebo materiálů za účelem klasifikace jejich obsahu. Označování informací pomáhá uživatelům rychle pochopit, čeho se informace týká a jak by s ní měli zacházet.

Ačkoliv zákon o archivnictví a spisové službě pracuje primárně s pojmem „dokument" a nikoliv informace, definuje dokument natolik široce (viz Box 8), že za něj lze považovat prakticky jakoukoliv zaznamenanou informaci. Povinnosti ze zákona podrobněji rozpracovává vyhláška o podrobnostech výkonu spisové služby.[42] Podle zákona o archivnictví a spisové službě mají všechny subjekty, které vykonávají spisovou službu, povinnost opatřit veškeré vytvořené dokumenty jednoznačným identifikátorem a zaevidovat je.[43] Zákon, ani vyhláška neukládají regulovaným subjektům povinnost vyznačovat na jimi vytvořených dokumentech stupeň důvěrnosti, a to bez ohledu na citlivost nebo kategorii informací, které obsahují. **Obecná povinnost orgánů státní správy vyznačovat na neutajovaných informací stupeň důvěrnosti tedy zavedena není.**

U některých dílčích kategorií citlivých neutajovaných informací existuje povinnost jejich původce tyto informace řádně identifikovat a označit (nikoliv však stupněm důvěrnosti). Například u dokumentů kategorie NATO UNCLASSIFIED nebo EU LIMITE zákon o archivnictví a spisové službě výslovně stanoví, že tyto dokumenty musí být opatřeny odpovídajícím označením („NATO UNCLASSIFIED", potažmo „EU LIMITE").[44] U osobních údajů vyplývá implicitní povinnost snadné identifikace a evidence z GDPR,[45] u zvláštních skutečností podle krizového zákona označují orgány krizového řízení krizové plány a jiné materiály obsahující zvláštní skutečnosti slovy „Zvláštní skutečnosti"

BOX 8: Definice dokumentu podle § 2 písm. e) zákona o archivnictví a spisové službě

„Každá písemná, obrazová, zvuková nebo jiná zaznamenaná informace, ať již v podobě analogové či digitální, která byla vytvořena původcem nebo byla původci doručena."

[40] Možnosti úpravy pravidel interními předpisy a jinými řídícími akty jsou nicméně omezeny účinnou právní úpravou, s níž musí být v souladu.
[41] Stav návrhu zákona k 1. 9. 2024: ukončeno mezirezortní připomínkové řízení; identifikační číslo v eKLEP: KORND4KLAAG6.
[42] Vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby.
[43] § 64 zákona o archivnictví a spisové službě.
[44] § 64a zákona o archivnictví a spisové službě; toto ustanovení však v kontextu zákona o archivnictví představuje výjimku, neboť tento právní předpis není určen k popisu kategorií informací/dokumentů, ale ke stanovení obecných principů nakládání s nimi ve spisové službě.
[45] Články 5, 24, 25 a 32 GDPR.

nebo zkratkou „ZS“.[46] V takovémto případě se však nejedná o vyznačení stupně důvěrnosti informace. Označení slouží ke snadnější identifikaci toho, že daná informace spadá do určité specifické kategorie, s níž je zpravidla spojena i speciální právní úprava regulující nakládání s těmito informacemi a přístup k nim.

Napříč veřejnou a státní správou existuje široká paleta systémů označování neutajovaných informací (orientační přehled viz Příloha 1). Úřady nejčastěji rozlišují mezi informacemi určenými pro sdílení s veřejností (označeny např.: „Pro všechny“, „Určené ke zveřejnění“, „Pro veřejnost“ nebo „Veřejné“) a informacemi neurčenými pro veřejnost (označeny například jako „Pro služební potřebu“ nebo „Interní“). Některé státní orgány dále vyčleňují speciální typ extra citlivých informací, ke kterým je přístup umožněn pouze na principu need-to-know[47] (Zde se používá např. označení „Chráněné“ nebo „Velmi citlivé“.).

Všechny, během přípravy Koncepce zkoumané, ústřední správní orgány do svého systému označování zapracovaly také povinnosti, které jim u dílčích kategorií informací pramení přímo ze zákona. Způsoby, jakými tak učinily, jsou různé. Zatímco v rámci jednoho resortu je například označení „Osobní údaje“ samostatnou kategorií (tj. dokument je označen pouze štítkem „Osobní údaje“), u jiného se jedná o speciální podkategorii, která se připojuje k obecnějšímu označení (například „Pro služební potřebu – Osobní údaje“ nebo „Chráněné – Osobní údaje“). Kromě nekompatibilních systémů označování představuje problém taktéž nedostatečnost a nedůslednost při označování samotném. Orgány státní správy nejsou ze zákona povinny vyznačovat na každou neutajovanou informaci stupeň důvěrnosti. Řada z nich sice ukládá tuto povinnost prostřednictvím interního předpisu, v praxi však nejsou tyto předpisy vždy dodržovány. K pochybení dochází nejčastěji na samém počátku životního cyklu informace – tedy na úrovni jejího původce**.**

3.6.2 Sdílení neutajovaných informací napříč státní správou a se soukromým sektorem

Efektivní a systematické sdílení informací je nezbytným předpokladem pro fungování moderní, dynamické a výkonné státní správy. Překážky ve sdílení vytváří komunikační a informační bariéru, která může vést ke zpomalení rozhodovacích procesů a navyšuje riziko přijímání nepřesných či neúplných rozhodnutí.

Stávající systém je dlouhodobě vnímán jako nevyhovující a nepodporující sdílení informací napříč státní správou. Hlavním důvodem je nejednotnost klasifikace a označování. Zatímco některé státní orgány mají ve svých interních předpisech stanoveno, jaké informace a za jakých podmínek je možné napříč státní správou sdílet, jiné nikoliv. Nejednotnost klasifikace a označování citlivých neutajovaných informací zároveň komplikuje, až znemožňuje, zavedení zautomatizovaných postupů a vytvoření jednotných zabezpečených systémů pro sdílení citlivých neutajovaných informací napříč státní správou. Části státní správy se rovněž potýkají s nedostatkem vzájemné důvěry mezi relevantními subjekty a s obavami z vynesení citlivých neutajovaných informací neoprávněným osobám.[48]

3.6.3 Ochrana citlivých neutajovaných informací

Chybějící jednotný přístup k citlivým neutajovaným informacím v rámci státní správy má zásadní negativní dopad na ochranu těchto informací. Absence definice vede k absenci identifikace, která následně způsobuje absenci jednotného označení a znemožňuje zavedení jednotných standardů jejich ochrany

[46] § 27 zákona o krizovém řízení.

[47] Princip "need-to-know" (princip nezbytné znalosti) je zásada z oblasti informační bezpečnosti a ochrany utajovaných či citlivých informací, která stanovuje, že ten, kdo nepotřebuje konkrétní informaci ke své práci, nesmí ji znát a naopak, kdo ke své práci tuto informaci potřebuje, znát ji musí, a to v úplnosti.

[48] Neoprávněnou osobou je v tomto kontextu myšlena osoba, která neměla pro přístup k dané informaci či nakládání s ní formální oprávnění.

a nakládání s nimi (např. stanovení vhodných komunikačních kanálů či nosičů, požadavky na případné šifrování a další aspekty související se zabezpečením).

Z vyjádření shromážděných během příprav Koncepce rovněž vyplynulo, že se některé státní orgány opakovaně potýkají s případy, kdy jeden státní orgán perspektivou jiného státního orgánu chybně vyhodnotí žádost o poskytnutí informace podle zákona o svobodném přístupu k informacím a zveřejní informaci (např. seznam kritické infrastruktury), která poskytnuta a zveřejněna být neměla.

Některé ústřední orgány státní správy se taktéž potýkají s velkým množstvím žádostí podle zákona o svobodném přístupu k neutajovaným informacím (zpravidla bezpečnostního charakteru), které považují za citlivé, avšak nelze je podřadit pod žádnou, v současné době existujících, výjimek z práva na poskytování informací. Při zpracování Koncepce tak byly zaznamenány apely na vytvoření nové výjimky, a to pro velmi úzkou množinu nejcitlivějších neutajovaných informací.

3.7 Shrnutí a závěry analýzy současného stavu

Státní správě ČR chybí jednotný, efektivní a uživatelsky přívětivý model klasifikace, označování, ochrany a sdílení citlivých neutajovaných informací.

Český právní řád rozeznává pouze informace utajované a dále dílčí skupiny citlivých neutajovaných informací (např. osobní údaje, důvěrné informace podle zákoníku práce nebo zvláštní skutečnosti). Existuje velká množina citlivých neutajovaných informací, které specificky rozeznávány a regulovány nejsou (např. citlivé interní resortní politiky, analýzy, neveřejná stanoviska a další). V ČR tak chybí jasná a v praxi použitelná obecná (zastřešující) definice citlivých neutajovaných informací. Definice chybí i na čistě koncepční, právně nezávazné úrovni.

Přes existenci obecných pravidel pro nakládání s dokumenty ve správním řádu a zákoně o archivnictví a spisové službě neexistuje v rámci státní správy ČR jednotný systém označování úrovně důvěrnosti neutajovaných informací. Pro některé dílčí kategorie informací (např. zvláštní skutečnosti) vyplývá tato povinnost ze zákona, není tomu však pro všechny kategorie neutajovaných informací. Praxe napříč státní správou je roztříštěná. Resorty a instituce zavádí prostřednictvím interních předpisů své vlastní, často nekompatibilní, systémy třídění a označování informací. Nejednotnost klasifikace a označování následně komplikuje sdílení informací napříč státní správou. Obvyklým problémem je také nedostatečná důslednost, kdy část vytvořených informací není jejich původci označena vůbec. Aktuální stav znemožňuje zavedení jednotných standardů ochrany a nakládání s neutajovanými citlivými informacemi. V praxi rovněž dochází k případům neúmyslného i úmyslného zpřístupňování citlivých neutajovaných informací neoprávněným osobám. Některé rezorty se rovněž potýkají s případy záměrného vyzrazování citlivých informací třetím stranám (např. v kontextu veřejných zakázek).

Subjekty regulované podle ZKB, tedy de facto všechny orgány státní správy, jsou povinny mít přehled o informacích, které zpracovávají jejich informační a komunikační systémy, ohodnotit důvěrnost těchto informací a přijmout opatření k jejich ochraně. Povinnosti a opatření podle ZKB a navazujících prováděcích předpisů nemohou samy o sobě nahradit jednotný systém ochrany, klasifikace, označování a sdílení citlivých neutajovaných informací. Představují nicméně užitečný základní stavební blok pro jeho vytvoření.

4 Vize a strategické cíle

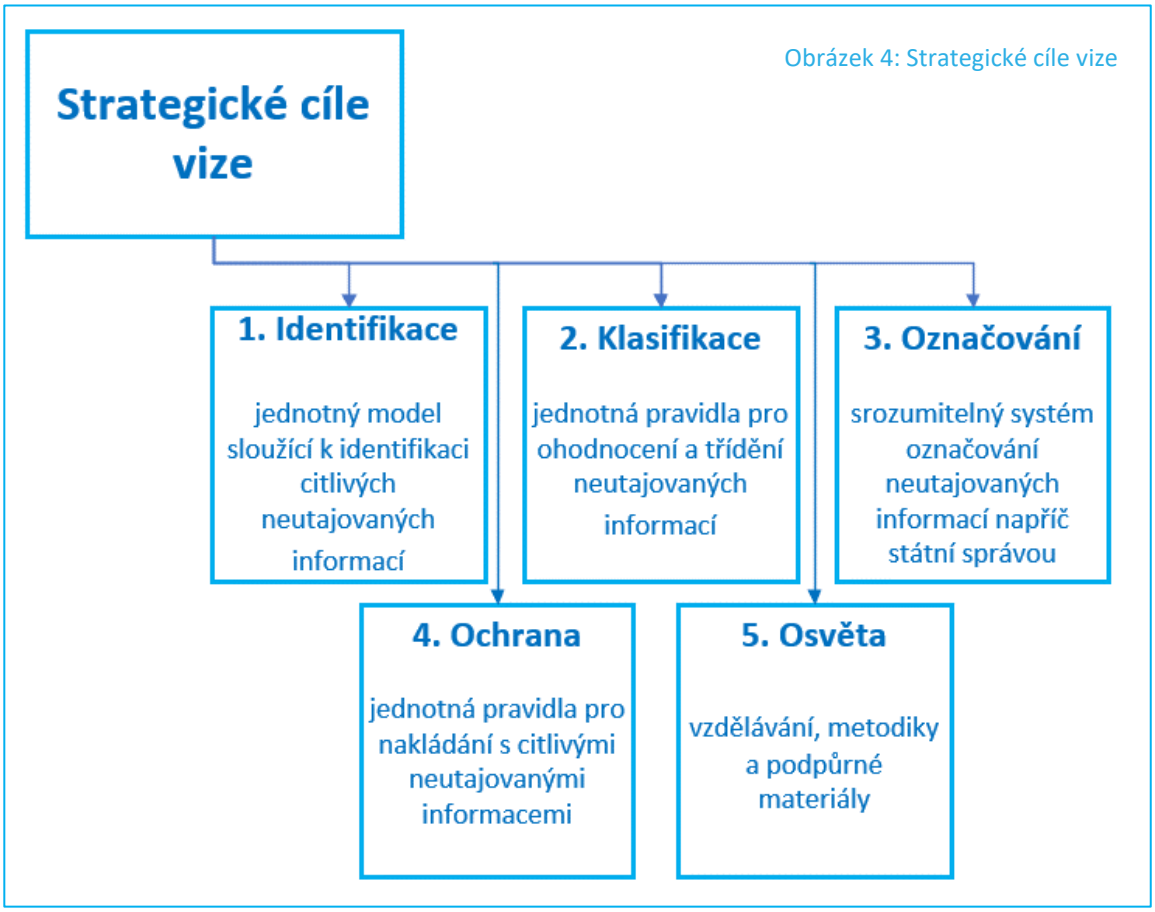
Řešení problematických aspektů současného stavu ochrany citlivých neutajovaných informací vyžaduje komplexní přístup. Ten se musí opírat o jasnou vizi a brát v úvahu postoje, zkušenosti a potřeby všech relevantních aktérů státní správy.

Navrhovaná vize: ČR bude mít efektivní, srozumitelný a uživatelsky přívětivý model ochrany, označování a sdílení citlivých neutajovaných informací, který bude široce využívaný a bude odpovídat soudobým požadavkům pro zpracování informací v informačních a komunikačních systémech.

Navrhovaná vize se opírá o pět strategických cílů, které jsou klíčové pro její dosažení. Co cíl, to dílčí oblast nezbytná k vytvoření funkčního a efektivního systému ochrany a sdílení (citlivých) neutajovaných informací. Jednotlivé cíle jsou vzájemně propojené a na sobě závislé (viz Obrázek 4).

Těmito dílčími oblastmi jsou:

I. **Identifikace**
II. **Klasifikace**
III. **Označování**
IV. **Ochrana**
V. **Osvěta**



Obrázek 4: Strategické cíle vize

Zdroj: NÚKIB

4.1 Strategický cíl č. 1: Vytvoření jednotného modelu sloužícího k identifikaci citlivých neutajovaných informací.

- **Cílový stav:** Bude vytvořen a zaveden jednotný model pro posouzení citlivosti neutajovaných informací sloužícího mj. k identifikaci vysoce citlivých neutajovaných informací.

4.2 Strategický cíl č. 2: Nastavení jednotných pravidel klasifikace neutajovaných informací v rámci státní správy.

- **Cílový stav:** Budou vytvořena a zavedena uživatelsky přívětivá a jednotná pravidla klasifikace neutajovaných informací v rámci státní správy.

4.3 Strategický cíl č. 3: Nastavení jednotných pravidel označování citlivých neutajovaných informací v rámci státní správy.

- **Cílový stav:** Budou vytvořena a zavedena uživatelsky přívětivá a jednotná pravidla označování neutajovaných informací v rámci státní správy. Bude nastaven takový systém označování informací, který umožní snadné rozpoznání toho, jaké informace a za jakých podmínek je možné sdílet mimo organizaci původce.

4.4 Strategický cíl č. 4: Nastavení jednotných pravidel ochrany a sdílení citlivých neutajovaných informací v rámci státní správy.

- **Cílový stav:** Budou vytvořena a zavedena jednotná pravidla pro nakládání s neutajovanými informacemi včetně přístupu k nim, jejich pozměňování, sdílení (včetně vhodných komunikačních kanálů), uchovávání, zabezpečení a ničení, která budou aplikovatelná napříč státní správou. Systém bude efektivní, srozumitelný a uživatelsky přívětivý. Bude odpovídat požadavkům moderních informačních a komunikačních systémů a bude kompatibilní s případným budoucím zapojením automatizačních procesů.

4.5 Strategický cíl č. 5: Aktivní osvěta a budování dobré praxe při nakládání s citlivými neutajovanými informacemi.

- **Cílový stav:** Bude kontinuálně a systematicky navyšováno povědomí o nakládání s citlivými neutajovanými informacemi mezi orgány státní správy, ale i soukromými subjekty a jejich zaměstnanci. Bude vypracována návodná metodika včetně praktických příkladů, která bude systematicky šířena zejména napříč státní správou.

5 Opatření a možné varianty řešení

K dosažení předložené vize a strategických cílů bude zapotřebí motivace a vůle na straně všech zainteresovaných subjektů, především pak na straně ústředních orgánů státní správy.

Na základě analýzy stávajícího stavu se k naplnění stanovené vize a strategických cílů navrhují níže popsané obecné varianty řešení. Tři varianty (A, B a C) se opírají o stejný jednotný model klasifikace, označování a nakládání s neutajovanými informacemi, ale liší se mírou právní závaznosti navrhovaných řešení, nutností přijmout legislativní změny a v celkové kapacitní a časové náročnosti jejich implementace v rámci státní správy. Čtvrtou možnou variantou je varianta nulová, která by znamenala zachování stávajícího stavu bez jakýchkoliv změn.

Popis navrhovaných variant řešení je úmyslně obecný. Cílem Koncepce jakožto strategického dokumentu je předložit základní model možného řešení, nikoliv finální detailní podobu. Předpokládá se, že zvolená varianta řešení bude po projednání a přijetí Koncepce Bezpečnostní radou státu (dále jen „BRS“) detailně rozpracována, upřesněna, zdokonalena a v případě potřeby taktéž upravena.

Hlavními cíli navrhovaných variant řešení (s výjimkou nulové) jsou:

1. **Identifikace:** Vytvoření jednotného modelu klasifikace neutajovaných informací, který umožní identifikaci citlivých neutajovaných informací.
2. **Klasifikace:** Zavedení jednotného systému třídění neutajovaných informací, který umožní snadné rozpoznání citlivých neutajovaných informací.
3. **Označování:** Zavedení jednotného systému označování neutajovaných informací, který umožní snadné rozpoznání citlivých neutajovaných informací.
4. **Ochrana:** Zavedení jednotných pravidel a standardů pro nakládání s neutajovanými informacemi, které posílí ochranu citlivých neutajovaných informací.
5. **Osvěta**: Vytvoření robustní metodické podpory a vedení při implementaci a následné aplikaci nového systému.

5.1 Model jednotného systému klasifikace, označování a nakládání s neutajovanými informacemi (stejný pro varianty A, B a C)

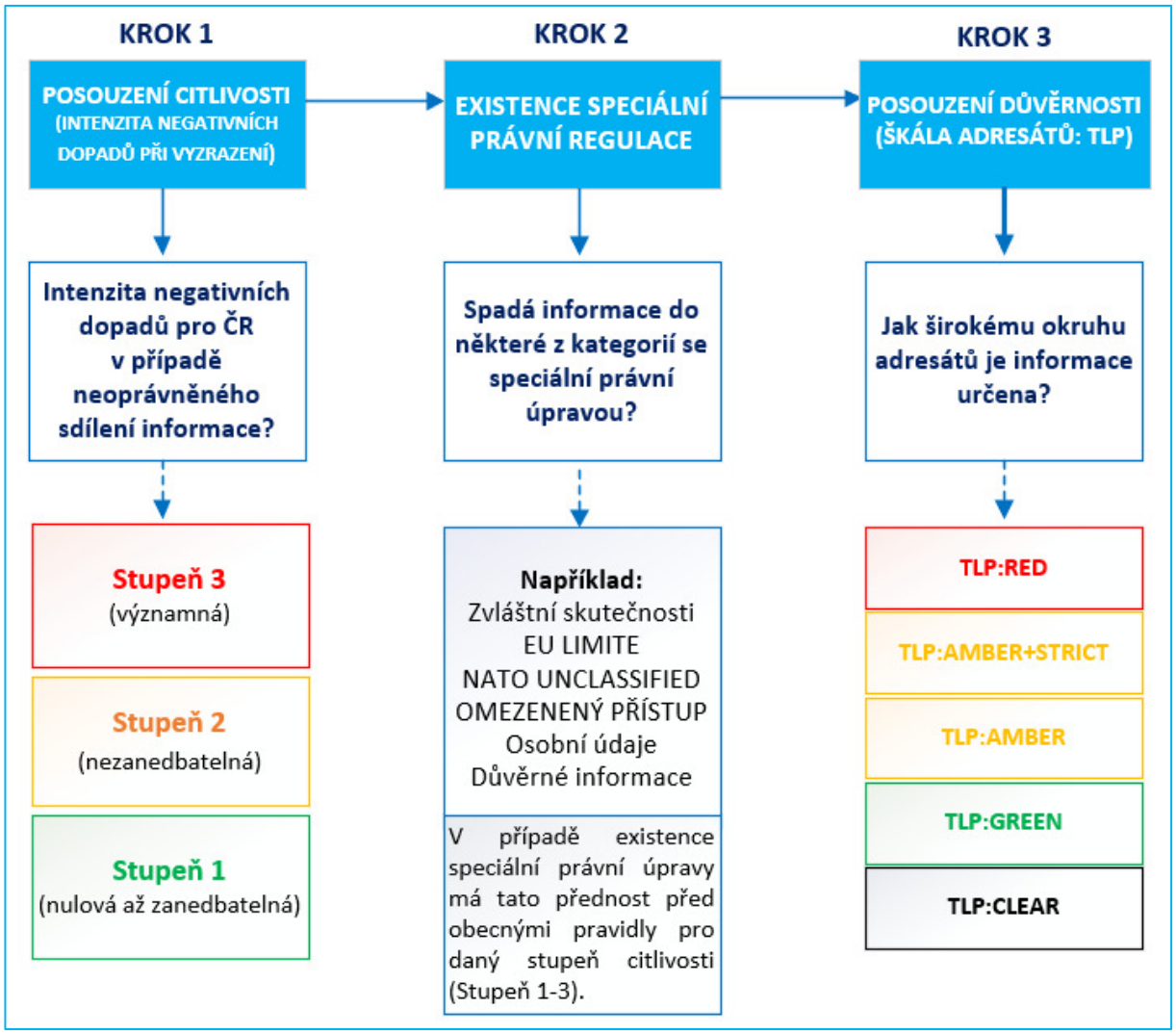
Varianty A, B a C navrhují vytvoření **jednotného systému klasifikace, označování a nakládání s neutajovanými informacemi**, který by byl aplikovatelný napříč státní správou. Základní model je pro všechny tři varianty obdobný. Varianty A a B se liší primárně rozsahem právní závaznosti a mírou legislativních změn. Varianta C představuje kombinaci variant A a B.

Navrhovaný model předpokládá vytvoření jednotného systému, který bude postaven na **posouzení neutajované informace na základě tří hlavních parametrů**:

1. **Stupeň citlivosti informace**, tedy intenzita nepříznivých dopadů pro ČR v případě vyzrazení nebo neoprávněného sdílení dané informace;
2. **existence speciální právní regulace**, která předepisuje pravidla pro nakládání s daným typem informací (např. úprava kategorie NATO UNCLASSIFIED“ podle § 64a zákona o archivnictví); a
3. **míra důvěrnosti informace**, reflektující šíři okruhu adresátů, kterým je informace určena.

Proces klasifikace informace podle nově navrhovaného modelu (viz Obrázek 5) kopíruje přirozenou myšlenkovou úvahu, která se od každého původce informace v rámci státní správy očekává již nyní. Tedy

posoudit: 1) Nakolik je nově vytvořená informace citlivá, 2) jakými právními normami je regulovaná a 3) s jakými subjekty je či není možné ji sdílet.



Obrázek 5: Orientační návrh procesu posouzení (klasifikace) informace Zdroj: NÚKIB

5.1.1 KROK 1: Citlivost informace

Míra citlivosti informace v kontextu představovaného modelu znamená míru intenzity nepříznivých dopadů způsobených ČR případným vyzrazením nebo neoprávněným poskytnutím předmětné informace. Neutajované informace by se na základě parametru citlivosti dělily do tří stupňů. **Níže uvedený popis jednotlivých stupňů je ilustrativním návrhem, který nikterak nepředurčuje finální definici.** Předpokládá se, že vymezení jednotlivých stupňů bude předmětem rozpracování v rámci implementace Koncepce po jejím schválení BRS.

- **Stupeň 3:** Neutajovaná informace, jejíž vyzrazení by pro ČR mělo významný nepříznivý dopad.
  - Nejcitlivější kategorie neutajovaných informací, které ze všech neutajovaných informací vyžadují nejvyšší míru ochrany. Zpravidla se bude jednat o velmi citlivé, avšak neutajované informace, interní analýzy či reporty.

3

- Výzvou pro další fázi projektu bude vytvoření precizní definice, která zajistí, že se bude pod tento stupeň podřazena pouze úzká množina neutajovaných informací a že tato kategorizace nebude nadužívána či zneužívána. Výzvou bude rovněž formulování definice, která nepovede k záměně se systémem utajovaných informací. Je žádoucí připomenout, že podle platné právní úpravy je utajovanou informací taková informace, jejíž vyzrazení nebo zneužití může způsobit zájmům ČR zákonem stanovenou míru újmy (materiální znak), a která je zároveň uvedena na seznamu utajovaných informací (formální znak). U stupně 3 se zavedení formálního znaku v podobě vytvoření seznamu chráněných informací nepředpokládá, odlišnost materiálního znaku utajovaných a citlivých neutajovaných informací ale je a bude i nadále výzvou.
- Lze se domnívat, že řada z informací náležících do této kategorie bude spadat do stávajících výjimek z práva na svobodný přístup k informacím. V případě zvolení právně závazné varianty zahrnující legislativní změny (varianta A) je otevřeno k diskusi, zda pro celou tuto úzkou kategorii velmi citlivých neutajovaných informací nezvážit zavedení nové, pečlivě formulované výjimky do zákona o svobodném přístupu k informacím.

- **Stupeň 2:** Informace, jejichž vyzrazení by pro ČR vedlo k nezanedbatelné nepříznivému dopadu.

2

- Kategorie informací, jejichž vyzrazení nebo neoprávněné poskytnutí, by vedlo k vyššímu než zanedbatelnému nepříznivému dopadu, avšak bez překročení hranice pro Stupeň 3.
- Do této kategorie bude spadat většina informací, které jsou nyní označovány jako „interní“ nebo „pro služební potřebu“. Tedy informace, které nejsou a priori určeny ke zveřejnění a je v zájmu státní správy mít přehled o jejich šíření (a toto případně podřídit určitým pravidlům).

- **Stupeň 1**: Veřejné/zveřejnitelné informace nebo informace, jejichž vyzrazení by vedlo pro ČR k nulovému či zanedbatelnému nepříznivému dopadu.

1

- Nejméně citlivá kategorie informací, které vyžadují nejnižší úroveň ochrany.
- Tato kategorie zahrnuje veřejné informace, informace určené ke zveřejnění nebo neveřejné informace, jejichž vyzrazení či poskytnutí neoprávněné osobě by vedlo k nulovým nebo zanedbatelným nepříznivým dopadům.

V souladu se strategickým cílem Koncepce č. 4 („nastavení jednotných pravidel ochrany a sdílení citlivých neutajovaných informací v rámci státní správy“) se navrhuje spojit s jednotlivými stupni citlivosti konkrétní pravidla a standardy pro řízení informací a nakládání s nimi, a to primárně v těchto oblastech:

- Evidence a přístup;
- pozměňování a sdílení;
- uchovávání, archivace (včetně výběru z archiválií) a ničení;
- změny klasifikace včetně deklasifikace po celý životní cyklus informace;
- označování;

- opatřování dokumentů v elektronické podobě metadaty, obsahujícími informace o úrovni jejich ochrany a uvolnitelnosti;[49] a
- volba vhodných komunikačních kanálů, požadavky na případné šifrování a další aspekty související se zabezpečením.

Specifikace těchto pravidel se bude odvíjet jednak od již platných zákonných a podzákonných požadavků a zavedených standardů, jednak od výsledků detailní analýzy aktuálního stavu, která by v ideálním případě měla v další fázi projektu (po projednání Koncepce BRS) proběhnout.

5.1.2 KROK 2: Existence speciální právní regulace

Dalším parametrem a zároveň druhým krokem v procesu klasifikace neutajovaných informací podle navrhovaného modelu je identifikace toho, zda předmětná informace spadá do některé z dílčích skupin citlivých neutajovaných informací se speciální právní regulací. Jako příklad lze uvést kategorie NATO UNCLASSIFIED podle zákona o archivnictví nebo zvláštní skutečnosti podle zákona o krizovém řízení, u kterých právní řád ukotvuje jak jejich definici, tak i označování a nakládání s nimi.

V kontextu navrhovaného modelu představuje správné podřazení informace pod jednu z již regulovaných skupin informací klíčový krok, neboť v takovém případě bude mít tato speciální právní úprava přednost před obecnými pravidly. Zároveň může například omezovat okruh možných adresátů, a tím být i zásadní pro správné vyhodnocení třetího parametru – důvěrnosti informace.

5.1.3 KROK 3: Posouzení důvěrnosti – určení škály adresátů

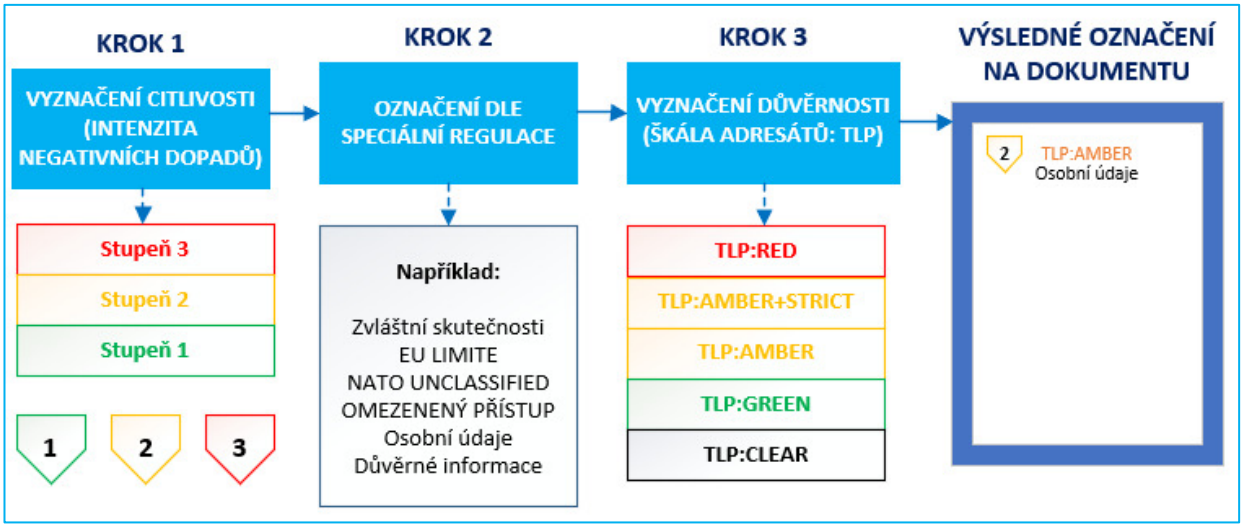
Posledním, třetím parametrem je důvěrnost informace a škála jejích adresátů. Jinými slovy, zodpovězení otázky, jak širokému okruhu adresátů je informace určena. Jedním z možných nástrojů pro posouzení a ohodnocení důvěrnosti informace je TLP protokol, který však využívá anglické pojmosloví a část státní správy s ním není plně obeznámena. O konkrétním nástroji bude s ohledem na potřeby české státní správy rozhodnuto v další části projektu.

Vyhodnocení důvěrnosti informace by mělo přirozeně vyplynout z vyhodnocení dvou předchozích parametrů – tedy míry citlivosti informace a jejího případného podřazení pod jednu ze speciálně regulovaných dílčích skupin citlivých neutajovaných informací.

5.1.4 Modelový návrh označování neutajovaných informací

Na základě vyhodnocení jednotlivých parametrů by byla předmětná informace doplněna o vyznačení citlivosti (zpravidla formou jednoduchého grafického znázornění nebo zápisu do metadat), šíře adresátů (např. prostřednictvím TLP) a případně také odpovídajícím označením podle speciální právní regulace (viz pro ilustraci Obrázek 6). Pro zjednodušení procesu a snížení administrativní zátěže by mohlo posloužit zavedení pravidla, podle kterého by se na neoznačené informace hledělo jako na dokumenty např. citlivosti Stupeň 2 a TLP:AMBER+STRICT. Pro většinu interních informací na úrovni Stupeň 2 a určeného pouze pro adresáty v rámci dané instituce (tj. informace přibližně na úrovni dnešního označení „Pro služební potřebu“ nebo „Interní“) by tak odpadla povinnost značení. Výsledné označení musí být přehledné a pro běžného uživatele snadno srozumitelné. V další fázi projektu by mělo být provedeno pilotní testování navrhovaného systému označování.

[49] S využitím principů podle IETF RFC 2634, 3114 a 5913, a ISO/IEC 15816:2002, rozpracovaných NATO v publikacích ADatP-4774 a 4778 a zakotvených v aliančních standardech STANAG 4774 a 4778, na které ČR přistoupila. V rámci této struktury se pro informace definují bezpečnostní klasifikace a bezpečnostní kategorie. V části popisu bezpečnostních kategorií informací se dále určují zájmové skupiny příjemců, pro které jsou informace uvolnitelné. Na základě nových právně zakotvených požadavků bude možné politiku následně aktualizovat.



Obrázek 6: Orientační návrh procesu označení informace na dokumentu Zdroj: NÚKIB

5.2 Varianta A: Vyžadující legislativní změny

- **Cílové subjekty:** Právně závazná pro celou veřejnou správu a příp. též soukromé subjekty prostřednictvím zákonem uložené povinnosti.
- **Implementace:** Tato varianta předpokládá legislativní změnu, ať již v podobě novelizace platných zákonů či vytvoření nového, pro oblast neutajovaných informací dedikovaného, zákona a příp. doprovodných podzákonných právních předpisů. Cílem této legislativní změny by bylo vytvoření výše popsaného jednotného systému klasifikace, označování a nakládání s neutajovanými informacemi a jeho ukotvení na úrovni zákona a podzákonných předpisů.
- **Subjekty zodpovědné za další rozpracování projektu a jeho implementaci:** MV, NÚKIB nebo MO jako hlavní gestor zodpovědný za koordinaci a vedení projektu ve spolupráci s ostatními dvěma úřady (tj. MO a NÚKIB, MV a MO, nebo MV a NÚKIB) a dalšími relevantními orgány státu.
- **Časový horizont:** Příprava návrhu legislativního řešení včetně doprovodných podzákonných předpisů a jeho předložení vládě do 31. prosince 2027.

Varianta A by vyžadovala přijetí následujících opatření:

- **Příprava a provedení legislativních změn:**
    - Hlavní cíl: Vytvoření jednotného systému klasifikace, označování a ochrany neutajovaných informací a jeho zavedení prostřednictvím legislativní změny, ať již formou nového legislativního předpisu nebo úpravou stávajících zákonů.
    - Provedení detailní analýzy sloužící k identifikaci konkrétních již existujících zákonů a podzákonných předpisů, které bude za účelem implementace projektu nutné novelizovat. Podle poznatků z analytické části Koncepce lze usuzovat, že případné změny by se mohly dotknout následujících právní předpisů:
        - Zákon o archivnictví; vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby; zákon č. 111/2009 Sb., o základních registrech; zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů;

vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy; správní řád; zákon o kybernetické bezpečnosti; a

- zákon o svobodném přístupu k informacím
    - Poskytnutí citlivé neutajované informace v důsledku chybného vyhodnocení podmínek podle zákona o svobodném přístupu k informacím nebo § 10a ZKB lze částečně předcházet efektivním metodologickým vedením a zvyšováním povědomí a úrovně znalostí v rámci státní správy. Součástí metodiky a metodologického vedení v rámci varianty A by tak byl důraz i na posilování znalosti zákona o svobodném přístupu k informacím a výjimek z práva na svobodný přístup k informacím napříč státní správou.
    - Je otevřeno k diskusi a analýze v další fázi projektu, zda u informací zařazených do Stupně 3, tedy pro tuto úzkou kategorii velmi citlivých neutajovaných informací, nezvážit zavedení nové pečlivě formulované výjimky do zákona o svobodném přístupu k informacím.
- Zohlednění plánovaných legislativních změn: Detailní návrh nového jednotného modelu by měl být kompatibilní s plánovanými legislativními změnami na národní i mezinárodní úrovni; například s návrhem zákona o správě dat a o řízeném přístupu k datům či s plánovaným Nařízení Evropského parlamentu a Rady o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie.

- **Analýza a revize standardů a technických aspektů:** Analýza stávajících standardů, norem a doporučení cílících na bezpečnost ochranu neutajovaných informací včetně technických aspektů s cílem identifikovat jaká míra a forma ochrany by se měla vztahovat na jednotlivé kategorie informací podle míry citlivosti (Stupeň 1 až 3).[50] Přijetí případných potřebných změn na úrovni legislativy i nezávazných doporučení.

- **Nelegislativní změny a práce:**
    - **Pilotní projekty:** Vytvoření efektivního a uživatelsky přívětivého systému bude vyžadovat pečlivé otestování plánovaných změn v rámci pilotních projektů ve vybraných a na pilotáži dobrovolně participujících úřadech státní správy.
    - **Technologická podpora:** Identifikace přesných požadavků na technologickou podporu a případné změny či úpravu ICT vybavení nezbytné pro zavedení nového jednotného systému.
    - **Metodické vedení:** Vypracování uživatelsky přívětivé metodiky včetně praktických příkladů.
    - **Osvěta a komunikační strategie:** Propagaci a šíření nově vytvořeného nástroje napříč státní správou. Důraz na dlouhodobou kultivaci prostředí. Vytvoření komunikační strategii, která bude informovat veřejnost a zaměstnance veřejné správy o změnách a jejich přínosech, čímž se zvýší povědomí a podpora nového systému.

Výhodou varianty A je možnost novelizovat právní řád tak, aby plně odpovídal potřebám nově vytvářeného modelu. Zásadní přidanou hodnotou je taktéž právní závaznost zavedených pravidel

[50] Příklad: K nejméně citlivým informacím (Stupeň 1) je možné přistupovat i z osobních zařízení, k informacím Stupně 3 pouze z pracovních.

pro širokou škálu subjektů, jimž by tak vznikla zákonná povinnost systém implementovat. Další výhodou je možnost závaznosti systému pro soukromoprávní subjekty (v případě nakládání s informacemi vytvořenými státní správou), což by napomohlo budování důvěry mezi státním a soukromým sektorem a ulevilo na administrativní zátěži při vzájemném sdílení informací. Varianta A rovněž otevírá možnost pro vytvoření sankčního mechanismu pro případy porušení nově zakotvených zákonných povinností.

Nevýhodou varianty A je její vyšší náročnost po stránce personálních, časových i finančních kapacit a tím pádem i vyšší zatížení orgánů státní správy. Implementace varianty A by vyžadovala změnu legislativy, relevantních podzákonných předpisů a administrativních postupů. V případě vytvoření sankčních mechanismů by bylo nutné vyřešit otázku jejich vymahatelnosti včetně určení dozorujícího orgánu a posílení jeho kapacit.

Varianta A umožňuje vytvoření efektivního, plnohodnotného, komplexního a právně závazného systému za cenu vyšší investice v podobě personálních, časových a finančních kapacit na straně státní správy.

5.3 Varianta B: Nevyžadující legislativní změny

- **Cílové subjekty:**
    - Státní správa s důrazem na ústřední správní orgány. Předpokládá se prvotní pilotní implementace v rámci bezpečnostně zaměřených resortů a následně rozšiřování napříč státní správou v závislosti na kapacitách a zájmu jednotlivých státních orgánů.
    - Po úspěšné pilotní implementaci by vláda ústředním orgánům státní správy uložila přistoupení do systému formou usnesení vlády. Pro další subjekty (včetně soukromoprávních) by bylo přistoupení k systému dobrovolné.
- **Implementace:** Tato varianta předpokládá vytvoření výše popsaného jednotného systému klasifikace, označování a nakládání s neutajovanými informacemi a jeho implementaci v míře možné bez změny stávající legislativy.
- **Subjekty zodpovědné za další rozpracování projektu a jeho implementaci:** MV, NÚKIB nebo MO jako hlavní gestor zodpovědný za koordinaci a vedení projektu ve spolupráci s ostatními dvěma úřady (tj. MO a NÚKIB, MV a MO, nebo MV a NÚKIB).
- **Časový horizont:** Příprava návrhu řešení do 31. prosince 2025. Provedení pilotního testování a předložení návrhu implementace nového modelu pro ústřední orgány státní správy vládě do 31. prosince 2026.

Varianta B předpokládá ponechání stávajícího právního stavu a přijetí následujících opatření:

- Vytvoření jednotného systému klasifikace, označování a nakládání s neutajovanými informacemi a jeho implementaci v míře možné bez změny stávající legislativy.
- Formulování právně nezávazných doporučení pro nakládání s neutajovanými informacemi citlivého povahy včetně přístupu k nim, jejich pozměňování, sdílení (včetně vhodných komunikačních kanálů), zabezpečení, uchovávání a ničení.
- Varianta B neumožňuje novelizaci zákona o svobodném přístupu k informacím. Klade proto důraz na metodologického vedení a posilování znalosti zákona a výjimek z práva na svobodný přístup k informacím v rámci státní správy. Metodologické vedení by rovněž obsahovalo doporučení konzultovat s původcem informace při posuzování žádostí o poskytnutí informací spadajících, co se posouzení citlivosti týče, do Stupně 3.

- Technologická podpora: Identifikace přesných požadavků na technologickou podporu a případné změny či úpravu ICT vybavení nezbytné pro zavedení nového jednotného systému.
- Vypracování uživatelsky přívětivé metodiky včetně praktických příkladů.
- Propagaci a šíření nově vytvořeného nástroje napříč státní správou. Důraz na dlouhodobou kultivaci prostředí. Vytvoření komunikační strategii, která bude informovat veřejnost a zaměstnance veřejné správy o změnách a jejich přínosech, čímž se zvýší povědomí a podpora nového systému.

Výhodou varianty B je absence potřeby legislativní změny. Varianta B je také flexibilnější, neboť předpokládá postupné zavedení nového modelu. Dává tak subjektům, pro které by byla skrze usnesení vlády povinná, možnost se na změnu postupně připravit, zatímco další subjektům (včetně soukromoprávních) umožňuje zapojení dobrovolné. Varianta B je finančně a kapacitně méně náročná, neboť nepředpokládá legislativní změnu a vytvoření nového dozorčího orgánu nebo rozšíření pravomocí orgánů již existujících.

Nevýhodou varianty B je její nevymahatelnost a s ohledem na absenci legislativního zásahu také omezený dopad, neboť nepovede k zavedení právně závazných pravidel pro pozměňování, sdílení, zabezpečení, uchovávání a ničení neutajovaných informací, pouze k formulaci doporučení. Hrozí, že v případě nízké motivace a nezájmu ze strany státní správy nebude nově vytvořený systém využíván, potažmo bude využíván pouze částí státní správy a jeho pozitivní dopad na stávající stav tak bude minimální.

Varianta B představuje kapacitně méně náročné a celkově více flexibilní řešení, existuje však značné riziko, že by její dopad byl velmi omezený a v konečném důsledku nevedl k zásadnímu zlepšení stávající situace.

5.4 Varianta C: Kombinovaná varianta – vytvoření provizorního systému a příprava legislativní změny

Varianta C navrhuje přednostní implementaci varianty B spolu s postupným zahájením prací na novém legislativním materiálu (varianta A).

- **Subjekty zodpovědné za další rozpracování projektu a jeho implementaci:** MV, NÚKIB nebo MO jako hlavní gestor zodpovědný za koordinaci a vedení projektu ve spolupráci s ostatními dvěma úřady (tj. MO a NÚKIB, MV a MO, nebo MV a NÚKIB) a dalšími relevantními orgány státu.
- **Časový horizont**: Příprava návrhu řešení prostřednictvím varianty B do 31. prosince 2025. Provedení pilotního testování a předložení návrhu implementace nového modelu pro ústřední orgány státní správy vládě do 31. prosince 2026. Předložení návrhu legislativních změn pro implementaci varianty A do 31. prosince 2027.

Výhodou varianty C je, že představuje kompromisní řešení, kdy finálním cílem je nezbytná legislativní změna, ale zároveň jsou zohledněny výrazné časové, personální a finanční kapacity, které příprava nového legislativního rámce přinese. Přednostní implementace varianty B může posloužit jednak pro provizorní přemostění období do přijetí legislativní změny, jednak jako příležitost pro identifikaci nejlepšího řešení a jeho otestování v praxi.

Nevýhodou varianty C je v celkovém měřítku větší množství investovaných kapacit a delší doba implementace všech částí této variant. Rovněž může dojít k situaci, kdy systémy vytvořené v rámci práce na variantě A (legislativní změna) a variantě B (nevyžadující změnu zákona) nebudou vzájemně kompatibilní a na sebe logicky navazující, což zkomplikuje přechod z varianty B na variantu A.

5.5 Nulová varianta: Ponechání stávajícího stavu

- **Cílové subjekty:** Celá státní správa.
- **Implementace:** Žádné kroky nejsou vyžadovány.

Nulová varianta přepokládá ponechání stávajícího stavu bez jakýchkoliv změn nebo vytváření nových nástrojů či systému klasifikace a označování citlivých neutajovaných informací.

Výhodou této varianty je nulové kapacitní, finanční i časové zatížení. **Nevýhodou** je ponechání současného dlouhodobě nevyhovujícího stavu. Na základě provedené analýzy a jejích závěrů se zvolení nulové varianty zásadně nedoporučuje.

5.6 Shrnutí a další postup

Všechny předkládané varianty řešení navrhují vytvoření jednotného systému klasifikace a označování citlivých neutajovaných informací a pravidel pro zacházení s nimi. Hlavním rozdílem mezi variantami A a B je míra závaznosti, robustnosti a vymahatelnosti nově vytvořeného systému. Varianta A je časově a personálně nejvíce náročná, zároveň by však její implementace vedla k trvalému, dlouhodobému, dostatečně robustnímu a kvalitnímu řešení. Varianta B představuje vůči orgánům státní správy vstřícnější a flexibilnější cestu. Implementace varianty B by umožnila postupné budování, testování a zavádění nově vytvořeného systému při současném zohlednění kapacit a potřeb jednotlivých státních institucí a rezortů. Varianta B však nepředstavuje dostatečně uspokojivé a dlouhodobě udržitelné řešení. Varianta C, kombinující obě varianty, by mohla být vhodným řešením pouze za předpokladu dostatečného a efektivního sladění obou fází.

Na základě výše uvedeného se doporučuje implementace varianty A, která ač časově a kapacitně náročnější, představuje nejpřímější a nejefektivnější cestu k dlouhodobému a dostatečně kvalitnímu řešení aktuálního stavu a vytvoření efektivního, komplexního a udržitelného systému ochrany citlivých neutajovaných informací.

Navrhuje se, aby **BRS společně se schválením Koncepce vybrala variantu A a uložila MV, jakožto hlavnímu gestorovi projektu, ve spolupráci s dalšími dvěma úřady (tj. NÚKIB a MO) rozpracování varianty A do podoby konkrétního řešení. To bude předloženo vládě v termínu do 31. prosince 2027** a následně postoupeno do legislativního procesu (viz Příloha 5: Návrh procesu implementace Koncepce).

6 Přílohy

Příloha č. 1: Ukázka systémů klasifikace a označování napříč různými subjekty

	Systém hodnocení důvěrnosti aktiv podle ZKB	Klasifikace informací podle interních předpisů	Označování informací podle vnitřních předpisů
Ministerstvo vnitra	1. Veřejné 2. Interní 3. Citlivé 4. Diskrétní	Napříč resortem nejednotné.	Napříč resortem nejednotné.
Ministerstvo obrany		1. Informace pro všechny 2. Informace pro služební potřebu 3. Osobní údaj 4. Důvěrná informace 5. Informace, která není určená ke zveřejnění	1. Bez označení 2. Informace pro služební potřebu. (Je možné doplnit upřesňujícím údajem – například „osobní údaje“.)
Ministerstvo zahraničních věcí	1. Veřejná informace (Nízká) 2. Interní informace (Střední) 3. Chráněné informace (Vysoká a kritická)		1. VEŘEJNÉ 2. INTERNÍ 3. CITLIVÉ 4. VYSOCE CITLIVÉ
Ministerstvo průmyslu a obchodu	1. Veřejné (C1) 2. Interní (C2) 3. Citlivé (C3) 4. Velmi citlivé (C4)		1. x 2. Pro vnitřní potřebu 3. Citlivé 4. Velmi citlivé
Národní úřad pro kybernetickou a informační bezpečnost	1. Nízká 2. Střední 3. Vysoká 4. Kritická		TLP protokol 1. CLEAR 2. GREEN 3. AMBER AMBER + STRICT 4. RED
Evropská unie (pouze Rada EU)	(neaplikuje se)		1. PUBLIC USE 2. EU LIMITE
Evropská unie (dle plánovaného nařízení EU-IBAs)	(neaplikuje se)	1. PUBLIC USE 2. NORMAL 3. SENSTIVE	1. PUBLIC USE 2. NORMAL 3. SENSTIVE
Severoatlantická aliance	(neaplikuje se)	1. NATO Releasable to Public 2. NATO Unclassified	1. NATO Releasable to Public 2. NATO Unclassified

Příloha č. 2: Informace poskytované Evropskou unií a Severoatlantickou aliancí

1. Evropská unie

Vzhledem k absenci právního předpisu, který by sjednocoval pravidla klasifikace a označování napříč institucemi, orgány a agenturami EU (dále jen „EU-IBAs)“, řeší organizační celky EU současnou situaci formou vlastních interních předpisů. Ty však nejsou navzájem plně kompatibilní a úprava je tak v rámci EU-IBAs značně roztříštěná.

Nejvýznamnější pro potřeby ČR je v tomto kontextu klasifikace, kterou používá Rada EU, její přípravné orgány, pracovní skupiny a výbory, a která pro označení citlivých neutajovaných informací používá značku „LIMITE“ (z francouzského „limité“ neboli omezený). Označení "LIMITE" se používá pro informace, které, ačkoli neutajované, jsou stále citlivé a vyžadují určitou míru důvěrnosti.[51] Typicky se jedná o návrhy, právní stanoviska nebo jiné interní dokumenty, které by mohly ovlivnit vyjednávání nebo jiné procesy, pokud by byly zveřejněny. Dokumenty označené jako „LIMITE" nejsou určeny pro širokou veřejnou distribuci, ale jsou omezeny na konkrétní příjemce v rámci institucí EU, členských států nebo jiných stran zapojených do konkrétních záležitostí.

Vzhledem k tomu, že se ČR zavázala neposkytovat informace označené jako „LIMITE“ třetí straně bez souhlasu původce, promítla tuto povinnost i do svého právního řádu, a to konkrétně do ustanovení § 64a odst. 1 zákona o archivnictví a § 11 odst. 1 písm. c) zákona o svobodném přístupu k informacím.

V současné době se na úrovni EU připravuje nařízení, jehož cílem je sjednotit pravidla informační bezpečnosti platná pro všechny EU-IBAs[52] (dále jen „návrh nařízení o informační bezpečnosti EU-IBAs“). Součástí navrhovaného nařízení o informační bezpečnosti EU-IBAs by měla být i úprava identifikace, klasifikace a označování utajovaných a neutajovaných informací. Návrh nařízení je projednáván Bezpečnostním výborem Rady, přičemž diskuse probíhá podle jednotlivých tematických klastrů. Projednávání kapitoly k ochraně neutajovaných informací bylo zahájeno na podzim 2023 a k červenci 2024 stále probíhají jednání. Po dlouhých diskusích a řadě připomínek členských států návrh směřuje k úpravě původně navrhovaných tří kategorií neutajovaných informací (PUBLIC USE, NORMAL a SENSITIVE) na pouze dvě kategorie: 1) PUBLIC a 2) INTERNAL NON-CLASSIFIED. Druhá kategorie by do budoucna nahradila dosavadní označení EU LIMITE. Zároveň by mohla být tato kategorie neutajovaných informací dále doplněna distribučním značením. Delegace se během jednání jasně vymezily proti kategorii citlivé neutajované informace, a to i z toho důvodu, že by mohlo často docházet k záměně s utajovanými informacemi, a to by vedlo k nižší ochraně utajovaných informací.

Ačkoliv návrh nařízení o informační bezpečnosti EU-IBAs neukládá povinnosti přímo členským státům EU, v praxi by jeho přijetí pro řadu zemí i tak znamenalo nutnost upravit své právní řády a systémy ochrany informací tak, aby byly s takto nově definovanými kategoriemi kompatibilní. Je žádoucí mít tento možný budoucí vývoj při vytváření nového modelu přístupu k citlivým neutajovaným informacím v ČR na paměti.

2. Severoatlantická aliance

Obdobnou kategorii jako EU LIMITE přestavují informace označené jako „NATO UNCLASSIFIED“, které s ČR sdílí NATO. I s těmito informacemi se může seznamovat pouze osoba, která je nezbytně potřebuje k výkonu své funkce, k pracovní nebo jiné obdobné činnosti. Jiným osobám může být takový dokument

[51] https://data.consilium.europa.eu/doc/document/ST-7695-2018-INIT/en/pdf

[52] Návrh nařízení Evropského parlamentu a Rady o bezpečnosti informací v orgánech, institucích a jiných subjektech Unie. Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union | European Commission (europa.eu).

poskytnut se souhlasem původce a za jím stanovených podmínek. Žádosti o zpřístupnění informací „NATO UNCLASSIFIED“ se v ČR podávají do rukou Národního bezpečnostního úřadu.[53]

Státní orgány, které pracují s dokumenty NATO UNCLASSIFIED, je zpravidla zařadí a přeznačí podle svých vlastních interních pravidel při zachování stejné míry ochrany. Ministerstvo obrany, tedy resort, který s informacemi NATO pracuje nejčastěji, kategorií „NATO UNCLASSIFIED“ řadí do kategorie „Pro služební potřebu“.

[53] Předpisy NATO vztahující se k ochraně utajovaných informací (nbu.cz)

Příloha č. 3: Příklady relevantní zahraniční úpravy

Spojené státy americké

Ve Spojených státech amerických (dále také „USA") funguje systém CUI vytvořený na základě dekretu prezidenta Baracka Obamy z roku 2010. Dohledovým orgánem je Národní archiv USA.[54]

Jako CUI se klasifikují takové neutajované informace, které vyžadují ochranu nebo je jejich šíření regulováno platnými zákony, předpisy či vládními politikami. Pod CUI program spadá řada kategorií včetně informací o kritické infrastruktuře (*Critical Infrastructure Information/CII*), kontrolovaných technických informací (*Controlled Technical Information/CTI*) nebo osobních údajů (*Privacy*). CUI jsou značeny štítkem „CUI" následovaným, v případě potřeby, upřesňující kategorií. Například „CUI: Privacy" nebo „CUI: For Official Use Only".

O informace spadající do kategorie CUI je možné požádat prostřednictvím Zákona o svobodě informací (*Freedom of Information Act*). Skutečnost, že je informace označena „CUI", nemá na posouzení žádosti o její poskytnutí vliv. Soukromoprávní subjekty pracující s CUI mají povinnost dodržovat pravidla pro jejich nakládání. Sankce za porušení těchto pravidel se odvíjí od závažnosti porušení a typu informace. Ty mohou být správněprávní i trestněprávní.

Belgie

Právně nezávazný pokyn k Federální politice bezpečnosti informací z roku 2019[55] rozděluje informace podle citlivosti do pěti kategorií: 0 (bílá), 1 (zelená), 2 (oranžová), 3 (červená) a 4 (černá). U každé kategorie je uvedeno, jaké informace pod ní spadají, zda, jak a kdy mají být označovány, jak mají být chráněny a kdo je oprávněn se s nimi seznamovat a nakládat. Součástí systému je grafické označení v podobě různě barevných zámků s číslem pro snadnou identifikaci příslušné kategorie.

- Informace kategorie „0" lze volně šířit. Poskytnutí těchto informací nezasahuje do zájmů organizací federální správy, služby nebo fungování skupiny pracovníků.
- Kategorie „1" je přiřazena těm informacím, jejichž nevhodné použití nebo šíření by pravděpodobně mělo dopad na zájem služby, ohrozilo fungování pracovníka nebo skupin osob v rámci jejich funkce v organizace nebo mělo dopad na soukromí jednotlivce či omezené skupiny osob. Informace kategorie „1" mohou být vyměňovány pouze tehdy, pokud je to nezbytné pro daný projekt a pouze s těmi externími subjekty, které jsou partnery daného orgánu a podepsaly dohodu o mlčenlivost. Veškeré informace používané a šířené v rámci organizací spolkové správy neoznačené jinou kategorií jsou automaticky považovány za informace kategorie „1".
- Do kategorie „2" spadají ty informace, jejichž nevhodné použití (například z důvodu nedostatečné ochrany dat) by poškodilo zájem federální organizace, kompromitovalo fungování služby či mělo vliv na soukromí skupiny osob nebo na soukromí zranitelných osob a/nebo dětí. Informace kategorie „2" jsou vyhrazeny pro omezenou skupinu spolupracovníků federálních správních organizací nebo pro konkrétní partnery.
- Kategorie „3" je přiřazena těm informacím, jejichž nevhodné použití by mohlo vážně poškodit klíčové zájmy federálních organizací nebo mělo vliv na soukromí skupiny osob nebo na soukromí

[54] Controlled Unclassified Information (CUI) | National Archives
[55] Federal Information Security Policy Guideline (belgium.be)

zranitelných osob a/nebo dětí. Dále do této kategorie spadají ty informace, jejichž neautorizované zveřejnění, úprava nebo zničení by mohly vytvořit významné riziko pro federální organizace. Jako příklad lze uvést data chráněná federálními nebo evropskými předpisy o ochraně soukromí a data chráněná dohodami o důvěrnosti. Informace kategorie „3“ musí být vždy označeny a přístup k nim je vyhrazen pro omezenou skupinu spolupracovníků federálních organizací nebo pro konkrétní partnery.

Grafické značení podle belgické federální politiky bezpečnosti

Zdroj: https://bosa.belgium.be/en

- Kategorie „4“ označuje utajované informace. Jedná se o data, materiál nebo např. technologie, jejichž znalost nebo využití by mohly vážně ohrozit fungování Belgie, mezinárodních institucí nebo bilaterálních, multilaterálních či mezinárodních dohod.

Austrálie

Hlavním policy dokumentem, který předkládá požadavky pro minimální akceptovatelnou úroveň zabezpečení důvěrnosti informací pro entity australské vlády je **Protective Security Framework Policy: Classification systém**.[56] Tento propracovaný dokument obsahuje podrobná závazná pravidla pro klasifikaci informací podle úrovně jejich důvěrnosti včetně pravidel pro jejich označování (např. označování různých datových nosičů nebo využití doplňujících štítků), manipulaci, pozměňování, sdílení a ničení. Součástí jsou taktéž tabulkové přehledy různých praktických příkladů a decision-tree pro snazší ohodnocování úrovně citlivostí informací.

			Security Classified Information			
	UNOFFICIAL	**OFFICIAL**	**OFFICIAL: Sensitive**	**PROTECTED**	**SECRET**	**TOP SECRET**
Při porušení důvěrnosti informace lze očekávat	**Žádný dopad**	**1. Nízký dopad**	**2. Nízký až střední dopad**	**3. Vysoký dopad**	**4.Extrémní dopad**	**5. Katastrofický dopad**
	Žádnou újmu Informace, které nejsou součástí výkonu úředních povinností.	**Žádnou nebo nevýznamnou újmu** Většina rutinních informací.	**Omezenou újmu** způsobenou jednotlivci, organizaci nebo vládě.	**Újmu** národnímu zájmu, organizacím nebo jednotlivcům.	**Vážnou újmu** národnímu zájmu, organizacím nebo jednotlivcům.	**Výjimečně vážnou újmu** národnímu zájmu, organizacím nebo jednotlivcům.

[56] PSPF Policy 8: Classification system v2018.8 (protectivesecurity.gov.au), Protective Security Policy Framework

Kanada

Kanadský systém rozděluje citlivé informace na utajované (*Classified*) a neutajované neboli Chráněné (*Protected*). „Chráněné" informace jsou takové, u nichž lze důvodně očekávat, že by v případě jejich ohrožení mohlo dojít k poškození jiného než národního zájmu, tj. individuálního zájmu, např. osoby nebo organizace.[57] Informace, v případě jejich vyzrazení by mohlo dojít k poškození národních zájmů, obrany a udržení sociální, politické a hospodářské stability Kanady, se klasifikují jako utajované.

Citlivé neutajované informace dělí kanadský systém do tří kategorií: Chráněné A (*Protected A)*, Chráněné B (*Protected B)* a Chráněné C (*Protected C)*. U každé z kategorií je stanoveno, kdo má k danému typu informací přístup a kde a za jakých podmínek mohou být uchovávány. Celý systém je ukotven v Zákoně o vládních institucích a v k němu náležející vyhlášce.[58]

Úroveň klasifikace	Popis	Příklad dopadů rizika
Veřejné	Informační aktiva, která nezpůsobí újmu jednotlivcům, vládám nebo institucím soukromého sektoru a finanční ztráta bude zanedbatelná.	Žádný minimální dopad. Žádné nebo minimální nepříjemnosti, pokud není k dispozici. Žádný nebo minimální dopad v případě ztráty nebo změny.
Chráněné A	Informační aktiva, která by v případě ohrožení mohla způsobit újmu jednotlivci, organizaci nebo vládě.	Nespravedlivá konkurenční výhoda. Narušení podnikání, pokud není k dispozici nebo je nedostupné.
Chráněné B	Informační aktiva, která by v případě ohrožení mohla způsobit vážnou újmu jednotlivým organizacím nebo vládě.	Ztráta pověsti nebo konkurenční výhody. Ztráta důvěry ve vládní program. Ztráta soukromí. Ztráta obchodního tajemství nebo duševního vlastnictví. Ztráta příležitosti (např. pojištění) Finanční ztráta.
Chráněné C	Informační aktiva, která by v případě ohrožení mohla způsobit mimořádně vážnou újmu jednotlivci, organizaci nebo vládě.	Ztráta života. Ztráta veřejné bezpečnosti. Významná finanční ztráta Kompromitace právního systému. Kompromitace jednání kabinetu. Zničení spojenectví a vztahů. Významné škody. Sabotáž/terorismus.

[57] Levels of security – Security screening for government contracts – Security requirements for contracting with the Government of Canada – Canada.ca (tpsgc-pwgsc.gc.ca)
[58] Data & Information Security Classification | AGLC

Spojené království Velké Británie a Severního Irska

Vláda Spojeného království Velké Británie a Severního Irska (dále jen „VB“) používá systém, který rozděluje informace na oficiální (*OFFICIAL*), tajné (*SECRET*) a přísně tajné (*TOP SECRET*). Do kategorie *OFFICAL* spadají neutajované informace, které vyžadují určitou úroveň ochrany z důvodu jejich citlivosti. Tyto informace jsou určeny pouze pro služební účely a neměly by být poskytovány neoprávněným osobám nebo subjektům. Kategorie *OFFICIAL* se dělí na dvě podkategorie: *OFFICIAL* a *OFFICIAL-SENSITIVE*. K těmto označením už se žádná další (např. PERSONAL) nepřidávají, pokud je nezbytná bližší specifikace, autoři dokumentu k němu mohou přiložit upřesňující pokyn.[59] Výjimky z práva na svobodný přístup k informacím stanovuje ve VB Zákon o svobodě informací z roku 2000 (*Freedom of Information Act*).[60] Označení informace jako *OFFICIAL* či *OFFICIAL-SENSITIVE* není automatickým důvodem pro zamítnutí žádosti o její poskytnutí. Každá informace musí být individuálně posouzená ve vztahu ke konkrétní žádosti. Ochranné značení může sloužit jako určitá indikace pro posuzující orgán, samo o sobě ale nemůže být rozhodujícím faktorem.[61]

	Typ informace	**Příklad informace**
Bez označení	Zveřejněné informace a informace ke zveřejnění	Veřejná oznámení a letáky, zveřejněné informace, informace, které neobsahují osobní údaje nebo jiný citlivý obsah, materiály určené ke školení.
OFFICIAL	Informace, které jsou produktem běžných operací a služeb veřejného sektoru, u kterých by zveřejnění v médiích nebo krádež mohlo mít škodlivé následky, ale které nepředstavují zvýšenou míru ohrožení.	Obecné správní záznamy, které nejsou určeny ke zveřejnění.
		Policy dokumenty, obchodní dokumenty nebo správní záznamy.
OFFICIAL-SENSITIVE	Informace obsahující osobní údaje	Dokumenty obsahující osobní údaje, jako jsou osobní záznamy, záznamy o občanech nebo pachatelích trestných činů.
	Zvlášť citlivé informace	Záznamy obzvlášť citlivých případů, sporné návrhy politik nebo doporučení, záznamy z citlivých jednání.
SECRET	Velmi citlivé informace, které odůvodňují zvýšená ochranná opatření na obranu před určenými nebo vysoce schopnými hrozbami.	Informace související s národní bezpečností a obranou, bojem proti terorismu nebo ochranou svědků.
TOP SECRET	Nejcitlivější informace vyžadující nejvyšší úroveň ochrany před nejvážnějšími hrozbami.	Ohrožení důvěrnosti informace by mohlo způsobit rozsáhlé ztráty na životech nebo ohrozit bezpečnost či hospodářský blahobyt státu nebo spojenců.

[59] Pokud by ohrožení mohlo způsobit rozsáhlé ztráty na životech nebo ohrozit bezpečnost či hospodářský blahobyt země nebo spřátelených států.
[60] Freedom of Information Act 2000 (legislation.gov.uk)
[61] information-provided-in-confidence-section-41.pdf (ico.org.uk)

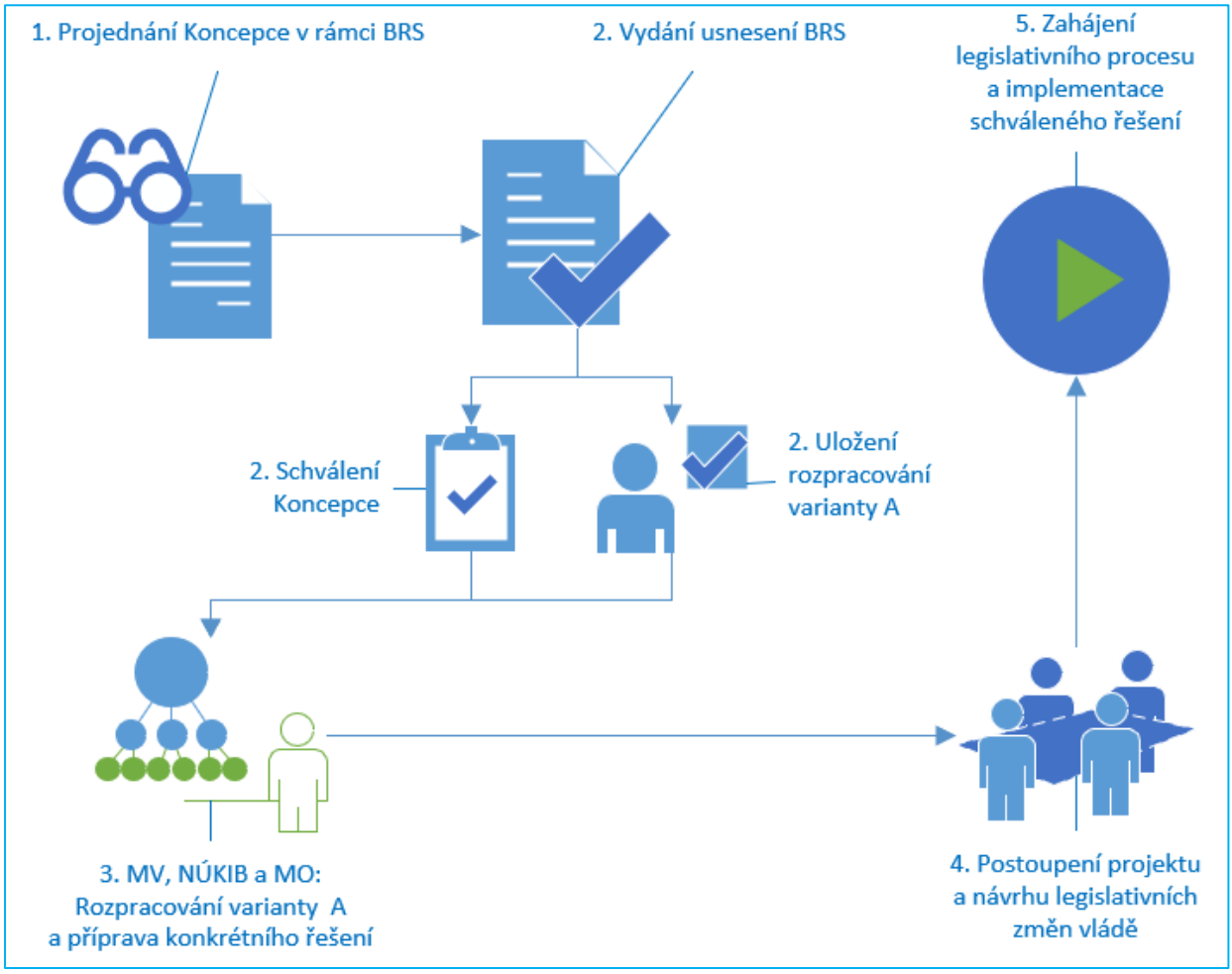
Příloha č. 4: Doporučovaná stupnice hodnocení důvěrnosti aktiv (Příloha č. 1 k platnému znění Vyhlášky o kybernetické bezpečnosti)

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. Traffic Light Protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.[62]	Není vyžadována žádná ochrana.
Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky pro řízení přístupu
Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Přenosy informací komunikační sítí jsou chráněny pomocí kryptografických prostředků.
Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.	Pro ochranu důvěrnosti jsou využívány prostředky, které zajistí řízení a zaznamenávání přístupu. Dále metody ochrany zabraňující zneužití aktiv ze strany administrátorů. Přenosy informací jsou chráněny pomocí kryptografických prostředků.

[62] Nejnovější verze Traffic Light Protocolu, TLP 2.0 vydaná v září 2022, používá místo TLP:WHITE označení TLP: CLEAR.

Příloha č. 5: Návrh procesu implementace Koncepce

1. Projednání Koncepce v rámci Bezpečnostní rady státu
2. Přijetí usnesení, kterým Bezpečnostní rada státu:
   a) Schvaluje Koncepci;
   b) vybírá z navržených řešení variantu A; a
   c) ukládá variantu A k rozpracování MV jakožto hlavnímu gestorovi a koordinátorovi projektu ve spolupráci s ostatními dvěma úřady (tj. MO a NÚKIB).
3. Pověřené státní orgány rozpracují variantu A a připraví návrh konkrétního řešení včetně návrhu potřebných legislativních změn (v termínu do 31. prosince 2027).
4. Předložení vypracovaného řešení vládě.
5. Zahájení legislativního procesu a implementace projektu.



7 Seznam zkratek

BIS – Bezpečnostní informační služba

BRS – Bezpečnostní rada státu

ČR – Česká republika

DIA – Digitální a informační agentura

EU – Evropská unie

ISMS – Information Security Management System

Koncepce – Koncepce ochrany neutajovaných informací citlivé povahy

MO – Ministerstvo obrany

MZV – Ministerstvo zahraničních věcí

MV – Ministerstvo vnitra

NATO – Severoatlantická aliance

NBÚ – Národní bezpečnostní úřad

NÚKIB – Národní úřad pro kybernetickou a informační bezpečnost

TLP – Traffic Light Protocol

ÚOOÚ – Úřad pro ochranu osobních údajů

ÚZSI – Úřad pro zahraniční styky a informace

VKB – Vyhláška o kybernetické bezpečnosti

VZ – Vojenské zpravodajství

ZKB – Zákon o kybernetické bezpečnosti

ZS – Zvláštní skutečnosti