ČESKÁ AGENTURA PRO STANDARDIZACI

BIM KONCEPCE

# Pravidla pro výměnu informací, které nemohou být umístěny v rámci řešení CDE

Datum: Listopad 2025

ČESKÁ AGENTURA PRO STANDARDIZACI

BIM KONCEPCE

**Vypracoval:**

Ing. Adam Ševčík

© Agentura ČAS 2025

Tento dokument může být bezplatně šířen v jakémkoliv formátu nebo na jakémkoliv nosiči bez zvláštního povolení, pokud nebude šířen za účelem zisku ani materiálního nebo finančního obohacení. Musí být reprodukován přesně a nesmí být použit v zavádějícím kontextu. Bude-li tento dokument znovu vydáván, musí být uveden jeho zdroj a datum zveřejnění. Všechny obrázky, grafy a tabulky mohou být použity bez povolení, pokud bude uveden zdroj.

Česká agentura pro standardizaci upozorňuje, že obsah předmětného dokumentu není konečný a bude podléhat dalším aktualizacím a zpřesněním, zejména pak v závislosti na výsledcích zpětné vazby v rámci realizace pilotních projektů a tvorby nové legislativy. Připomínky České republiky – Ministerstva obrany byly zapracovány/vysvětleny, ale zapracování/vysvětlení nebylo akceptováno. Přesto Česká republika – Ministerstvo obrany vyslovilo souhlas s vydáním dokumentu. Případný uživatel předmětného dokumentu, nechť užívá dokument s vědomím, že se nejedná o jeho úplnou a konečnou verzi a nelze vyloučit, že se obsah předmětného dokumentu ještě v čase výrazněji změní a doplní.

# OBSAH

1 ÚVOD ..... 4

2 DIGITÁLNÍ BEZPEČNOSTNÍ HROZBY ..... 5

3 ZÁKLADNÍ PRÁVNÍ RÁMEC ..... 8

3.1 Národní bezpečnostní úřad ..... 8

3.2 Národní úřad pro kybernetickou bezpečnost ..... 8

3.3 Úřad pro ochranu osobních údajů (ÚOOÚ) ..... 8

3.4 European Union Agency for Cybersecurity (ENISA) ..... 9

3.5 SHRNUTÍ ..... 9

4 OBECNÁ PRAVIDLA PRO VÝMĚNU UTAJOVANÝCH INFORMACÍ ..... 10

Interní předpisy a organizační opatření ..... 10

Oprávnění k přístupu a kontrola uživatelů ..... 10

Technická a fyzická bezpečnost ..... 11

Pokyny pro předávání a sdílení informací ..... 11

Školení, kontrola a vyvozování odpovědnosti ..... 11

4.1 Varianta A: Utajované a neutajované informace v rámci CDE ..... 11

4.2 Varianta B: CDE nebude sloužit pro tok utajovaných informací ..... 12

5 SHRNUTÍ Z POHLEDU ZÁKONA Č. 320/2001 SB. ..... 13

6 ZÁVĚR ..... 14

# 1 ÚVOD

Výměna informací ve stavebnictví je nedílnou součástí celého životního cyklu stavby, od přípravy a projektování, přes realizaci až po správu a údržbu vlastního majetku. Řízení a správa informací včetně využívání metody BIM prostřednictvím konceptu společného datového prostředí (CDE) významně přispívá k efektivnímu sdílení a správě informací.

Existují však specifické situace, kdy z technických, legislativních či bezpečnostních důvodů není možné ani vhodné všechny informace umístit v rámci společného datového prostředí (CDE), které je tvořeno běžně dostupnými nástroji.

Tato metodika proto stanovuje pravidla, jakým způsobem má být s takovými informacemi nakládáno v rámci povinností veřejného zadavatele jako povinné osoby, aby byla zajištěna jejich správná výměna a bezpečnost bez použití nástrojů společného datového prostředí.

Účelem metodiky je poskytnout doporučení a návod pro postup veřejných zadavatelů a ostatních účastníků investičního procesu při nakládání s informacemi, ke kterým se z různých důvodů nemůže přistupovat jako k běžné součástí informačního modelu stavby spravovaného pomocí společného datového prostředí.

Jedná se o informace obsahující citlivá (informace, které jsou pro veřejného zadavatele klíčové a současně druh těchto informací je upraven ve vnitřním předpisu veřejného zadavatele) či utajovaná data. Přestože tyto informace většinou nebudou přímo uloženy a sdíleny pomocí běžně dostupného nástroje společného datového prostředí, jejich existence a vazba na ostatní informace v podobě informačních kontejnerů musí být vždy zajištěna tak, aby byla zachována kontinuita a dohledatelnost celého informačního modelu stavby.

Tento dokument se proto zaměřuje na vymezení toho, jaké typy informací nemusí být součástí společného datového prostředí dle § 9 odst. 3) zákona č. 330/2025 Sb.

§ 9 Zákona odst. (3)

- Pokud je součástí informačního modelu stavby nebo jeho části utajovaná informace podle jiného právního předpisu, nemusí být součástí společného datového prostředí, pokud by takovým postupem mohlo dojít k porušení právních předpisů vztahujících se k ochraně utajovaných informací.

Důraz je kladen na bezpečnostní opatření veřejného zadavatele a jeho zaměstnanců, a jednoznačnou identifikaci citlivých informací v procesech řízení a správy informací.

Výsledkem je soubor pravidel, která podporují efektivní digitální spolupráci a zároveň zohledňují právní, bezpečnostní i technické limity současné praxe s důrazem na zachování bezpečnosti státu.

# 2 DIGITÁLNÍ BEZPEČNOSTNÍ HROZBY

Práce s informacemi o stavbě prochází díky digitalizaci různými změnami. Tyto změny jsou současně podporovány i legislativně prostřednictvím zákona 330/2025 Sb. Tento zákon v § 4 odst. 2) ustanovuje, že informační model stavby je pořizován a udržován ve společném datovém prostředí.

Dle § 2 odst. e) zákona

**Společné datové prostředí** je soubor

- nástrojů a
- požadavků

prostřednictvím kterých se

- uchovává,
- spravuje a
- sdílí

obsah informačního modelu stavby nebo jeho části.

S rostoucí digitalizací však zároveň dochází k výraznému nárůstu digitálních bezpečnostních hrozeb, které mohou negativně ovlivnit kvalitu, důvěryhodnost a dostupnost sdílených informací. Zvláště citlivé informace – například dokumentace kritické infrastruktury, citlivá technická řešení či osobní údaje – vyžadují zvýšenou pozornost, protože jejich únik nebo zneužití může mít zásadní dopady nejen na konkrétní projekt, ale i na bezpečnost státu.

**Obecně jsou oblasti se zvýšenou rizikovostí v důsledku digitalizace následující:**

- **Kybernetické útoky**

Jedním z nejčastějších a zároveň nejzávažnějších rizik jsou cílené kybernetické útoky. Ty se mohou projevovat různými způsoby – od phishingových e-mailů, které se snaží od uživatelů vylákat přístupové údaje, až po sofistikované útoky typu ransomware, které dokážou ochromit nástroje společného datového prostředí tím, že zašifrují data a znemožní jejich používání. Útočníci mohou mít zájem na průmyslové špionáži nebo sabotáži projektu. V případě velkých veřejných zakázek představuje takový útok nejen ekonomické riziko, ale i hrozbu pro národní bezpečnost, protože může vést k odhalení plánů kritické infrastruktury či energetických sítí.

- **Vnitřní hrozby**

Velmi významným problémem je také hrozba zevnitř. Na rozdíl od klasických kybernetických útoků, které přicházejí z vnějšího prostředí, se zde jedná o zneužití přístupu osobami, které mají do systému legální vstup. Tento typ hrozby může mít podobu vědomého jednání (např. kopírování dat při odchodu zaměstnance

z veřejného sektoru do privátního subjektu) i nevědomých chyb (např. nahrání neověřeného souboru obsahujícího malware). Protože se jedná o oprávněné uživatele, je jejich jednání obtížně odhalitelné a často se zjistí až ve chvíli, kdy dojde k úniku citlivých dat.

- **Nesprávné řízení přístupových práv a identit**

Další zásadní oblastí je nesprávné řízení přístupových práv a identit. Projekty, ve kterých je zapojeno velké množství účastníků – od investorů, přes projektanty, zhotovitele, subdodavatele, až po správce budovy – generují obrovské množství dat. Pokud není nastaven jasný systém rolí a oprávnění, může dojít k tomu, že se k citlivým dokumentům dostanou osoby, které je nemají mít k dispozici. To nejen ohrožuje bezpečnost, ale zvyšuje i riziko chyb a nesouladu.

- **Nedostatečné zabezpečení přenosu a ukládání dat**

Velmi aktuálním rizikem je i nedostatečné zabezpečení přenosu a ukládání dat. V této souvislosti je třeba sledovat i otázku geografického umístění dat – zda jsou ukládána v rámci České republiky, Evropské unie nebo mimo ni. Uložení mimo EU s sebou přináší právní komplikace zejména z pohledu ochrany osobních údajů a dodržování legislativy (např. GDPR).

- **Nedostupnost dat**

Neméně významnou hrozbou je i nedostupnost dat, ať už v důsledku technických problémů nebo záměrného útoku. Pokud se projekt spoléhá na centrální úložiště nástroje CDE, jakýkoli výpadek systému může zastavit práci celého týmu. Útoky typu DDoS (Distributed Denial of Service) mohou znepřístupnit platformu na několik hodin či dní, což může mít fatální dopady na plnění termínů projektu. Podobně i porucha hardwaru nebo softwaru bez dostatečných záloh může vést ke ztrátě dat, která jsou pro realizaci stavby klíčová.

- **Rizika spojená s archivací a kompatibilitou**

V oblasti dlouhodobé práce s daty je třeba zmínit rizika spojená s archivací a kompatibilitou. Stavební projekty mohou trvat mnoho let a data je potřeba uchovávat i po dokončení realizace stavby pro účely správy objektu. Pokud nejsou nastavena pravidla pro uchovávání dat, jejich formátovou kompatibilitu a pravidelnou migraci na nové technologie, hrozí, že se některé informace stanou v budoucnu nečitelné nebo nenávratně ztracené.

- **Lidský faktor**

Za pozornost stojí i **lidský faktor**, který bývá nejslabším článkem bezpečnosti. I nejlépe zabezpečené společné datové prostředí v podobě souboru nástrojů může být ohroženo, pokud uživatelé nedodržují základní bezpečnostní zásady, jako je pravidelná změna hesel, neotevírání podezřelých příloh atd. Útočníci často využívají lidské nepozornosti, nezkušenosti nebo důvěřivosti, aby se dostali k citlivým datům. V prostředí stavebních projektů, kde se účastní mnoho různých subjektů, se tímto způsobem mohou stát zranitelnými i ty části projektu, které jsou technicky dobře zabezpečené.

Všechny tyto hrozby ukazují, že zabezpečení citlivých informací v společném datovém prostředí je komplexní problém, který vyžaduje nejen technická řešení, ale také jasně nastavené procesy a odpovědnosti. Nestačí pouze nasadit technologii – je nutné, aby všichni účastníci projektu byli řádně proškoleni a rozuměli tomu,

jak bezpečně s informacemi pracovat.

**Pouze kombinace technických opatření** (šifrování, autentizace, zálohování, monitoring) **a organizačních pravidel** (řízení přístupů, smluvní povinnosti, odpovědnost jednotlivých rolí) dokáže zajistit, že digitální spolupráce v rámci společného datového prostředí bude skutečně bezpečná, udržitelná a odolná vůči stále sofistikovanějším kybernetickým hrozbám.

# 3 ZÁKLADNÍ PRÁVNÍ RÁMEC

Jak už bylo uvedeno výše, společné datové prostředí je dle zákona v podobě souboru nástrojů a požadavků hlavním prostředkem pro řízení a správu informací v rámci informačního modelu stavby.

Přesto existují určité kategorie dat, které z důvodu právních omezení, požadavků národní a evropské bezpečnosti či bezpečnostních rizik, nesmějí být spravovány pomocí běžných nástrojů společného datového prostředí.

Jedná se zejména o kategorii dat v podobě dokumentů a souborů klasifikovaných jako utajované informace. Tyto informace musí být uloženy a spravovány v prostředích, která splňují zvláštní podmínky ochrany a jejich správa podléhá přísným právním a technickým předpisům. Umístění takových dat do běžného nástroje společného datového prostředí by představovalo zásadní bezpečnostní riziko – od možnosti sabotáže kritické infrastruktury, přes únik osobních údajů, až po ztrátu kontroly nad softwarem. Z toho důvodu je nutné předem provést klasifikaci všech dokumentů a jasně stanovit, které informace jsou pro správu v rámci společného datového prostředí vhodné, a které naopak musí být spravovány v odděleném režimu.

## 3.1 Národní bezpečnostní úřad

V České republice je klíčovým orgánem pro oblast ochrany utajovaných informací Národní bezpečnostní úřad (NBÚ). Ten zajišťuje implementaci a dohled nad dodržováním následující legislativy:

- **Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti,**

který stanovuje pravidla pro nakládání s informacemi klasifikovanými jako:

- „vyhrazené“,
- „důvěrné“,
- „tajné“ a
- „přísně tajné“.

NBÚ vydává prováděcí vyhlášky, provádí bezpečnostní prověrky osob i organizací a určuje podmínky pro certifikovaná úložiště.

## 3.2 Národní úřad pro kybernetickou bezpečnost

V oblasti kybernetické bezpečnosti hraje hlavní roli Národní úřad pro kybernetickou a informační bezpečnost (NÚKIB), jehož působnost vymezuje:

- **Zákon č. 264/2025 Sb., o kybernetické bezpečnosti.**

NÚKIB dohlíží na ochranu informačních a komunikačních systémů veřejné správy a kritické infrastruktury, vydává vyhlášky a metodiky, provádí bezpečnostní cvičení a koordinuje reakci na kybernetické incidenty.

## 3.3 Úřad pro ochranu osobních údajů (ÚOOÚ)

Dalším dozorovým orgánem je Úřad pro ochranu osobních údajů (ÚOOÚ), který dohlíží na dodržování ochrany osobních údajů dle:

- **Zákon č. 110/2019 Sb., o zpracování osobních údajů a evropského nařízení GDPR**

Tento zákon vychází z:

nařízení Evropského parlamentu a Rady (EU) 2016/679 – GDPR, které stanovuje obecná pravidla pro ochranu

osobních údajů a na úrovni Evropské unie je základním právním rámcem pro ochranu informací a dat.

Do projektů s povinností pořizování informačního modelu stavby v společném datovém prostředí může vstoupit zákon č. 110/2019 Sb. zejména tehdy, pokud jsou v projektové dokumentaci a dalších informačních kontejnerech zpracovávány osobní údaje fyzických osob, které podléhají zvláštním režimům ochrany.

V závislosti na charakteru projektu mohou mít specifické pravomoci také Policie ČR a zpravodajské služby.

## 3.4 European Union Agency for Cybersecurity (ENISA)

V oblasti kybernetické bezpečnosti je hlavní evropskou agenturou ENISA (European Union Agency for Cybersecurity), která poskytuje metodiky, směrnice a podporu členským státům i jednotlivým organizacím. Z hlediska vyšetřování incidentů a prevence mezinárodní kriminality se uplatňuje i Europol, zejména jeho jednotka EC3 (European Cybercrime Centre). V případě projektů, které zasahují do obranných nebo přeshraničních záležitostí, je nutné také zohlednit bezpečnostní politiky Evropské obranné agentury (EDA) a relevantní rámce spolupráce NATO, pokud se projekt týká společné bezpečnosti a obrany.

V oblasti kybernetické bezpečnosti hraje zásadní roli

- **Směrnice (EU) 2022/2555 – NIS2,**

která harmonizuje požadavky na kybernetickou bezpečnost v členských státech a zavádí povinnosti pro provozovatele kritické infrastruktury a důležité informační systémy.

Pokud jde o utajované informace, Evropská unie pracuje s režimem EUCI (EU Classified Information), který stanovuje čtyři stupně klasifikace:

- „Restricted“,
- „Confidential“,
- „Secret“ a
- „Top Secret“.

## 3.5 SHRNUTÍ

Z výše uvedeného vyplývá, že informace, které nemohou být umístěny do běžného (neutajovaného) nástroje společného datového prostředí, jsou přesně vymezeny jak českou, tak evropskou legislativou.

V českém kontextu se jedná především o zákon č. 412/2005 Sb. a zákon č. 264/2025 Sb., které spolu s činností NBÚ a NÚKIB určují pravidla pro nakládání s utajovanými a citlivými informacemi. Na evropské úrovni pak pravidla GDPR, NIS2 a EUCI stanovují rámec ochrany osobních údajů, kybernetické bezpečnosti a klasifikovaných informací.

# 4 OBECNÁ PRAVIDLA PRO VÝMĚNU UTAJOVANÝCH INFORMACÍ

Stěžejným sdělením této kapitoly by mělo být, že veřejný zadavatel je při nakládání s utajovanými informacemi povinen postupovat zejména v souladu s právními předpisy České republiky.

Nedílnou součástí je i dodržování evropských nařízení a směrnic, pokud se na nakládání s utajovanými informacemi vztahují.

Každý zaměstnanec nebo smluvní partner, který se k informacím dostává, musí být předem seznámen s těmito povinnostmi a jejich porušení je postihováno jak pracovněprávně, tak trestněprávně. K docílení žádaných výsledků by měl přispět soubor obecných pravidel a doporučení vztahujících se k jednotlivým prvkům procesu zavádění, užívání a kontrolování dodržování bezpečnostně-orientovaného přístupu k správě informací o stavbě.

## Interní předpisy a organizační opatření

Veřejný zadavatel je povinen přijmout a udržovat aktuální soubor interních předpisů a organizačních opatření, která detailně popisují pravidla pro nakládání s utajovanými informacemi.

Tyto předpisy musí jasně definovat:

- odpovědnosti jednotlivých pracovníků,
- procesy pro přístup a autorizaci,
- mechanismy kontroly a dohledu nad dodržováním bezpečnostních opatření.

Součástí těchto dokumentů jsou i interní směrnice pro:

- klasifikaci informací,
- označování informací,
- ukládání informací,
- archivaci informací a
- likvidaci informací.

Veřejný zadavatel je také povinen pravidelně aktualizovat tyto předpisy v návaznosti na legislativní změny a technologický vývoj a zajistit, aby všichni zaměstnanci byli s aktuální verzí řádně obeznámeni.

## Oprávnění k přístupu a kontrola uživatelů

K utajovaným informacím mohou mít přístup pouze osoby, které splnily zákonné podmínky pro seznámení, zejména absolvovaly bezpečnostní prověrku u Národního bezpečnostního úřadu (NBÚ) nebo byly poučeny v souladu s příslušnou úrovní utajení.

Veřejný zadavatel musí vést evidenci všech osob s přístupem k utajovaným informacím, přičemž tato evidence musí být pravidelně kontrolována a aktualizována.

Současně musí být zavedena opatření pro pravidelné vyhodnocování rizik a kontrolu oprávnění, aby se zamezilo neoprávněnému přístupu.

Každé porušení přístupových pravidel musí být bezodkladně hlášeno, vyšetřeno a musí být přijata odpovídající nápravná opatření.

### Technická a fyzická bezpečnost

Pro výměnu a uchovávání utajovaných informací je nezbytné zajistit odpovídající technické a fyzické prostředí. To zahrnuje používání certifikovaných technických prostředků, šifrování při elektronické komunikaci, bezpečné datové sítě a zařízení splňující bezpečnostní standardy.

V oblasti fyzické bezpečnosti musí veřejný zadavatel disponovat zabezpečenými místnostmi a archivy, kontrolovaným vstupem do prostor, kamerovým systémem a předepsanými úrovněmi ochrany. Každý prostředek určený k přenosu či uchovávání utajovaných informací musí být pravidelně testován a auditován, aby byla zajištěna jeho plná funkčnost a shoda s právními a bezpečnostními požadavky.

### Pokyny pro předávání a sdílení informací

Předávání utajovaných informací mezi jednotlivými útvary veřejného zadavatele, případně mezi zadavatelem a externími subjekty, musí probíhat výhradně v souladu s předem schválenými postupy a pokyny. To zahrnuje volbu odpovídajícího způsobu přenosu.

Veškeré předání musí být zaznamenáno v příslušné evidenci a musí být dohledatelné, aby byla zajištěna odpovědnost všech zúčastněných stran.

Externí příjemci informací jsou povinni předem doložit odpovídající oprávnění a podepsat dohodu o ochraně informací, přičemž odpovědnost za dodržování předpisů nese i zadavatel jako původce informace.

### Školení, kontrola a vyvozování odpovědnosti

Veřejný zadavatel je povinen zajistit pravidelná školení všech zaměstnanců, kteří přicházejí do styku s utajovanými informacemi.

Školení se zaměřují nejen na právní a organizační rámec, ale i na praktické postupy bezpečného nakládání s informacemi.

Zároveň je nutné provádět pravidelné i mimořádné interní kontroly, audity a bezpečnostní prověrky, aby bylo možné odhalit případné nedostatky a okamžitě je napravit.

V případě porušení stanovených pravidel musí být vždy vyvozena odpovědnost – od kázeňských opatření až po oznámení případu příslušným orgánům činným v trestním řízení. Tímto způsobem zadavatel posiluje kulturu bezpečnosti a předchází opakování chyb.

**Pro projekty vyžadující pořizování informačního modelu stavby v společném datovém prostředí dle §4 odst. 2) zákona to v praxi znamená, že každá organizace (veřejný zadavatel) musí provést klasifikaci informací například v podobě dokumentů, vyhodnotit jejich charakter a rozhodnout, zda mohou být součástí společného datového prostředí a ukládány v jeho nástrojích nebo zda musí být ukládány v certifikovaných nástrojích pod dohledem NBÚ, NÚKIB či evropských bezpečnostních institucí.**

**Tímto způsobem se zajistí, že procesy digitální spolupráce budou bezpečné, právně v souladu a odolné proti současným i budoucím hrozbám.**

## 4.1 Varianta A: Utajované a neutajované informace v rámci CDE

Veřejný zadavatel musí před zpřístupněním konkrétního nástroje nebo nástrojů společného datového prostředí pro ukládání a správu všech (včetně režimových) informací zajistit, že tento nástroj ve formě softwaru **a jeho provoz jsou plně v souladu s platnou bezpečnostní legislativou**.

To zahrnuje definici kategorií utajení, postupy pro autorizaci přístupu a povinnosti všech uživatelů. Veřejný zadavatel musí rovněž zajistit smluvně nebo v technických specifikacích, že poskytovatel nástroje CDE je schopen garantovat odpovídající úroveň bezpečnosti, včetně šifrování, zálohování, monitoringu a auditních protokolů. Bez těchto opatření není možné utajované informace do nástroje CDE bezpečně ukládat.

Pro práci s utajovanými informacemi v nástroji CDE musí veřejný zadavatel zavést přísný systém řízení přístupu, který zohledňuje úroveň utajení jednotlivých dokumentů a oprávnění jednotlivých uživatelů. Každý uživatel musí být předem prověřen a oprávněn k nakládání s utajovanými informacemi v souladu s příslušnou bezpečnostní prověrkou.

Je povinen také zajistit evidenci všech přístupů, pravidelnou revizi oprávnění a možnost okamžitého zablokování účtu v případě podezření na narušení bezpečnosti. Systém musí podporovat jasnou identifikaci každého zásahu do dokumentu, aby byla zajištěna plná odpovědnost za manipulaci s informací. **Toto se týká také poskytovatele softwaru a třetí strany (např. zhotovitele).**

Veřejný zadavatel musí zavést soubor technických a organizačních opatření, která zajišťují ochranu utajovaných informací v nástrojích společného datového prostředí.

To zahrnuje bezpečné šifrování dat při přenosu i uložení, segmentaci přístupu podle úrovně utajení, zabezpečené zálohování, monitoring bezpečnostních událostí a pravidelný audit systému.

Dále je nutné stanovit vnitřní pokyny pro používání nástroje CDE včetně pravidel pro nahrávání, stahování a sdílení utajovaných dokumentů. Všechny tyto kroky musí být dokumentovány a pravidelně aktualizovány v souladu se změnami legislativy a technologického prostředí.

## 4.2 Varianta B: CDE nebude sloužit pro tok utajovaných informací

Přístup, správa a bezpečnostní opatření pro tok běžných informací se nikterak neliší oproti práci v jiných obvyklých a zavedených systémech veřejného zadavatele. To zahrnuje registraci uživatelů, definici rolí, a oprávnění, evidenci aktivit a pravidelnou aktualizaci přístupových práv. Technická opatření, jako jsou zálohování, zabezpečený přenos dat a ochrana proti malwaru, musí být přiměřená citlivosti informací, avšak nemusí dosahovat úrovně ochrany požadované pro utajované dokumenty. Důležité je rovněž zajistit školení uživatelů o správném používání nástroje CDE a zacházení s dokumenty, aby byla minimalizována rizika ztráty nebo nesprávného zpracování dat.

K tomuto „standardnímu režimu“ bezpečnostně orientovaného přístupu může být využita norma ČSN EN ISO 19650-5 — Bezpečnostně orientovaný přístup k managementu informací, která mimo jiné, poskytuje možnosti, jak postupovat při rozhodování a citlivosti informací a jejich správě.

# 5 SHRNUTÍ Z POHLEDU ZÁKONA Č. 320/2001 SB.

Z pohledu zákona č. 320/2001 Sb. o finanční kontrole je efektivní správa dokumentů a informací klíčová pro správné rozhodování a kontrolu veřejných prostředků.

Ukládání pouze běžných informací v nástrojích CDE umožňuje jednoduchou a rychlou evidenci, vyhledávání a sdílení dokumentů mezi pracovníky, bez nutnosti zajišťovat nákladné a administrativně náročné bezpečnostní prověrky a zvláštní technologická opatření.

Naopak zahrnutí utajovaných informací do společného datového prostředí výrazně komplikuje procesy, zpomaluje přístup k datům a vyžaduje dodatečné kontroly a omezení, které snižují celkovou efektivnost systému (toto sdělení se nevztahuje na subjekty osvobozené od povinnosti pořizováni a udržování informačního modelu stavby dle zákona č. 330/2025 Sb.).

Zákon o finanční kontrole současně klade důraz na účelnost – tedy na to, aby opatření odpovídala cíli, který veřejný zadavatel sleduje. Pokud společné datové prostředí, jako soubor nástrojů, slouží pro běžnou administrativu a řízení stavebních projektů, ukládání utajovaných informací je neúčelné, protože přináší složité požadavky na šifrování, monitoring a autorizace (včetně pořízení nástroje CDE – softwaru – v speciálním bezpečnostním režimu), které jsou v tomto kontextu nadbytečné. Ukládání pouze běžných dokumentů a informací umožňuje přiměřené a cílené využití systému, přičemž jsou zachovány všechny potřebné funkce pro podporu rozhodování a kontrolu finančních toků.

Z hlediska hospodárnosti znamená ukládání utajovaných informací v režimovém nástroji CDE vyšší náklady na technické zabezpečení, provozní dohled, audit a školení zaměstnanců. Každé zpřísnění přístupových práv a každá dodatečná kontrola zvyšuje časovou a finanční náročnost správy dokumentů a informací. Naopak varianta s běžnými informacemi minimalizuje tyto náklady a umožňuje efektivní využití stávajících technologií a lidských zdrojů, aniž by byla ohrožena správnost, úplnost nebo dohledatelnost informací potřebných pro finanční kontrolu.

Je zřejmé, že pro zajištění efektivnosti, účelnosti a hospodárnosti (neplatí pro subjekty osvobozené od povinnosti pořizováni a udržování informačního modelu stavby dle zákona č. 330/2025 Sb.) je vhodné v rámci společného datového prostředí ukládat primárně pouze běžné, neutajované informace.

Práce s utajovanými informacemi pomocí společného datového prostředí přináší značnou administrativní zátěž a finanční nároky, aniž by významně přispěla ke kvalitě finanční kontroly nebo rozhodování.

**Proto se doporučuje využívat společné datové prostředí v podobě souboru nástrojů pro běžnou dokumentaci projektů a administrativu a pro utajované informace zvolit oddělené a legislativně zajištěné systémy s odpovídajícími bezpečnostními opatřeními dle vnitřních předpisů organizace.**

# 6 ZÁVĚR

Výměna informací v rámci stavebních projektů využívajících s povinností pořizování informačního modelu stavby v společném datovém prostředí (CDE) představuje klíčový prvek pro efektivní správu a transparentní spolupráci. Tento dokument proto stanovuje základní a obecná pravidla pro nakládání s informacemi, které z technických, legislativních či bezpečnostních důvodů nemohou být kdykoliv umístěny v rámci souboru nástrojů společného datového prostředí.

Cílem této metodiky je upozornit veřejného zadavatele na utajované informace o stavbě (např. nakládání s informacemi o utajované místnosti), zajistit bezpečnou správu, dohledatelnost a kontinuitu v rámci informačního modelu stavby, a to zejména u citlivých a utajovaných dat. Veřejní zadavatelé tak mají k dispozici metodiku, která jim umožňuje jednotný a systematický přístup k těmto informacím, čímž se minimalizují rizika spojená s jejich zneužitím či ztrátou. **Zásadní výzvou při digitalizaci stavebnictví je zajištění bezpečnosti dat v prostředí rostoucích kybernetických hrozeb**. Tato metodika zdůrazňuje potřebu kombinace technických opatření, jako je šifrování a zabezpečený přenos dat, s organizačními pravidly, včetně přísného řízení přístupových práv a školení zaměstnanců.

**Oddělené systémy pro ukládání informací (běžné a utajované) jsou doporučovány jako efektivní a hospodárné řešení, které snižuje administrativní zátěž a zvyšuje bezpečnost.**

Pro veřejné zadavatele je klíčové provést předem klasifikaci dokumentů a jasně vymezit, které informace lze v nástrojích CDE spravovat a které vyžadují zvláštní režim.

V případě zvláštního režimu, musí veřejní zadavatelé dbát na to, aby informace byly spravovány současně na režimovém softwaru. Tímto způsobem lze zajistit soulad s právními předpisy a zároveň zachovat efektivitu digitální spolupráce.

Doporučení směřují k tomu, aby společné datové prostředí sloužilo primárně pro běžnou dokumentaci a administrativu a tok informací o stavbě, zatímco utajované informace by měly být ukládány v certifikovaných úložištích, a současně, aby s nimi bylo pracováno v jiném režimu.

Tento dokument tak přispívá k budování bezpečné a transparentní digitální spolupráce ve stavebnictví. Pravidelná aktualizace postupů, školení uživatelů a důsledné dodržování bezpečnostních opatření jsou nezbytné pro minimalizaci rizik a zajištění dlouhodobé udržitelnosti procesů správy informací o stavbě. V souladu s tímto přístupem lze efektivně řídit stavební projekty, chránit citlivé informace a **podporovat bezpečnost státu v digitálním věku**.

ČESKÁ AGENTURA PRO STANDARDIZACI

BIM KONCEPCE

Česká agentura pro standardizaci
Biskupský dvůr 1148/5, 110 00 Praha 1

Tel: +420 221 802 802
e-mail:
info@agenturacas.gov.cz
e-mail:
bim@agenturacas.gov.cz

www.agenturacas.gov.cz
www.KoncepceBIM.gov.cz