PORTÁL NÚKIB

Bezpečná likvidace informací a dat

Režim vyšších povinností

TLP:CLEAR

25. května 2026

Verze 1.0

Národní úřad pro kybernetickou a informační bezpečnost

Co se dozvím v tomto dokumentu?

Tento podpůrný materiál k zákonu č. 264/2025 Sb., o kybernetické bezpečnosti a vyhlášce č. 409/2025 Sb., o bezpečnostních opatřeních poskytovatele regulované služby v režimu vyšších povinností (dále jen „VBO-V“), představuje praktické vodítko pro bezpečnou likvidaci informací a dat, jejich kopií a technických aktiv, která jsou jejich nosiči. Dozvíte se, jaké způsoby likvidace informací a dat jsou přípustné a pro jaké typy aktiv je vhodné je použít. Dokument slouží jako praktický návod, který pomůže organizacím zajistit, aby likvidace informací a dat probíhala bezpečně, prokazatelně a v souladu s požadavky VBO-V.

Pokud máte jakékoliv další otázky, podívejte se na www.portal.nukib.gov.cz nebo nám napište na regulace@nukib.gov.cz.

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

Informace obsažené v dokumentu se vztahují k právní úpravě účinné ke dni platnosti publikované verze dokumentu.

1 Pravidla a postupy pro určení způsobu likvidace informací a dat, jejich kopií a technických nosičů

Likvidací se rozumí odstranění, přepsání, nebo fyzická likvidace informací a dat, jejich kopií a technických nosičů tak, aby po vyřazení zařízení nedošlo k neoprávněnému zpřístupnění nebo zneužití těchto informací a dat.

Dle § 3 odst. c) VBO-V povinná osoba provádí přiměřená bezpečnostní opatření směřující k zajištění kybernetické bezpečnosti regulované služby na základě cílů systému řízení bezpečnosti informací, bezpečnostních potřeb a řízení rizik.

Pravidla likvidace informací a dat musí být nastavena přiměřeně důležitosti jednotlivých aktiv. To v praxi znamená volit takové postupy, které odpovídají charakteru informací, dat, typu nosiče, hrozbám i možnostem organizace, aniž by ji neúměrně zatěžovaly. Organizace musí rozumět důležitosti a hodnotě svých informací a dat a dopadům případného zneužití, aby mohla určit, zda postačí běžné odstranění, bezpečné přepsání, nebo je nutná fyzická likvidace nosiče.

Stanovená pravidla musí být v praxi dodržována a jejich dodržování musí být vynucováno.

Cílem je, aby likvidace informací a dat probíhala bezpečně, prokazatelně a úměrně rizikům, která jsou s aktivem spojena. Pravidla a postupy musí být kompatibilní i s dalšími právními předpisy, které mohou ukládat specifické požadavky na likvidaci určitých typů aktiv.

Povinnost organizace definovat a uplatňovat vhodné způsoby likvidace informací a dat, jejich kopií a technických aktiv, která tato data obsahují, je stanovena v příloze č. 2 VBO-V pro oblast likvidace informací a dat.

Způsob likvidace musí vždy odpovídat hodnocení a úrovni aktiv podle přílohy č. 1 VBO-V. Organizace proto musí mít jasně stanovená pravidla a postupy, které určují, jakým způsobem budou jednotlivé úrovně a typy aktiv likvidovány.

Při tvorbě těchto pravidel je nutné zohlednit zejména:

- hodnotu úrovně aktiv z hlediska důvěrnosti informací,
- technologii a typy nosičů,
- míru kontroly organizace nad aktivem (zda je nosič fyzicky pod kontrolou organizace),
- zda se aktivum nachází v dedikovaném nebo sdíleném prostředí,
- kdo bude likvidaci provádět (interní pracovník vs. externí dodavatel),
- dostupné kapacity a zdroje (technické, lidské, finanční),
- dostupné způsoby likvidace,
- aktuální stav nosiče, protože poškozené nosiče mohou vyžadovat jiný způsob likvidace než běžně funkční.

Při posuzování citlivosti sdílených informací a dat a s tím související důvěrností, může organizace zohlednit také pravidla označování informací podle verze mezinárodního standardu tzv. Traffic Light Protocol (TLP), který je podrobně popsán zde: Národní úřad pro kybernetickou a informační bezpečnost – sdílení informací.

Organizace musí mít pravidla pro likvidaci informací, dat a technických aktiv formálně stanovena v bezpečnostní politice a související bezpečnostní dokumentaci. Tato dokumentace musí být pravidelně přezkoumávána, aktualizována a promítána do provozních postupů. Organizace je povinna se těmito pravidly řídit a zajistit, aby byla součástí běžného provozu a byla dostupná všem osobám, které se na likvidaci aktiv podílejí.

1.1 Pravidla a postupy likvidace informací a dat z pohledu řízení dodavatelů

Pokud jsou informace, data nebo technická aktiva umístěna mimo přímou kontrolu organizace (např. v prostředí dodavatele poskytujícího cloudové služby nebo outsourcing), musí být způsob jejich likvidace smluvně stanoven. Pravidla musí odpovídat úrovni aktiva dle přílohy č. 1 VBO-V a být v souladu s požadavky přílohy č. 2 VBO-V.

Organizace stanoví požadované způsoby likvidace informací a dat (odstranění, přepsání, fyzická likvidace) s ohledem na jejich hodnotu, citlivost a míru rizika. Dodavatel musí provést likvidaci způsobem, který odpovídá úrovni hodnocení aktiva, je bezpečný, přiměřený a umožňuje prokázání jejího provedení.

Smluvní ustanovení by měla řešit zejména:

- způsob, jakým dodavatel likviduje informace a data po ukončení služby,
- jak bude organizace informována o provedené likvidaci dat a jak bude prokazatelně doložena,
- postupy pro nakládání se zálohami, kopiemi a obdobnými soubory,
- pravidla pro fyzickou likvidaci aktiv prováděnou dodavatelem,
- možnost provedení kontroly plnění smluvních podmínek.

Organizace je povinna průběžně ověřovat, že dodavatel provádí likvidaci v souladu s požadavky a v návaznosti na řízení aktiv dle § 7 VBO-V.

V režimu vyšších povinností musí organizace stanovit a dokumentovat přesná pravidla pro likvidaci informací a dat, jejich kopií a technických aktiv podle úrovně aktiv. Tyto postupy musí vycházet z hodnocení aktiv, reflektovat jejich hodnotu, technologii, umístění, kontrolu a stav, a určovat konkrétní způsoby likvidace.

1.2 Způsoby likvidace informací a dat, jejich kopií a technických aktiv, která jsou nosiči informací a dat

a) **Odstranění**: Znepřístupnění dat (např. smazání souboru, reset zařízení do továrního nastavení, vyhození nosiče do odpadu). Data mohou být obnovitelná při vynaložení určitého úsilí. Použitelné pro úroveň hodnocení aktiva **Nízká.**

b) **Přepsání:** bezpečné vymazání uložiště vhodným nástrojem (opakované přepsání informací a dat náhodnými hodnotami nebo bezpečná likvidace kryptografických klíčů použitých k zašifrování informací a dat). Nevhodné pro poškozené, nepřepisovatelné nosiče a nosiče nešifrované s velkou paměťovou kapacitou. Volně dostupné nástroje neumožňují obnovení po násobném přepsání dat a informací. Použitelné pro úroveň hodnocení aktiva **Nízká** až **Vysoká**.

c) **Fyzická likvidace**: Nezvratné zničení nosiče mechanickým, chemickým nebo tepelným působením. Data nelze obnovit ani při značném úsilí. Použitelné pro úroveň hodnocení aktiva **Nízká** až **Kritická**.

Tabulka č. 1: Příklady možných způsobů likvidace

🟢 Nízká úroveň hodnocení aktiva 🟡 Střední úroveň hodnocení aktiva
🟠 Vysoká úroveň hodnocení aktiva 🔴 Kritická úroveň hodnocení aktiva

Typ nosiče informací	Odstranění	Přepsání	Fyzická likvidace
Informace v listinné podobě (např. tištěné dokumenty, psané poznámky, ruční zápisy)	Vyhození do odpadu 🟢	–	Skartace, spálení 🟢🟡🟠🔴
Datová média (např. magnetické pásky, HDD, SSD, USB flash disk, paměťové karty)	Smazání dat, formátování média 🟢	Přepsání dat, bezpečné vymazání úložiště vhodným nástrojem 🟢🟡🟠	Mechanické zničení nosiče dat 🟢🟡🟠🔴
Nepřepisovatelná optická média (např. CD-R, DVD-R, BD-ROM)	Vyhození do odpadu 🟢	–	Rozstříhání, skartace 🟢🟡🟠🔴
Přepisovatelná optická média (např. CD-RW, DVD-RW, BD-RE)	Smazání dat 🟢	Přepsání dat, bezpečné vymazání úložiště vhodným nástrojem 🟢🟡🟠	Rozstříhání, skartace 🟢🟡🟠🔴
Mobilní a koncová zařízení (např. počítače, telefony, tablety, IoT)	Reset zařízení do továrního nastavení 🟢	Přepsání dat, bezpečné vymazání úložiště vhodným nástrojem 🟢🟡🟠	Mechanické zničení zařízení nebo nosiče dat 🟢🟡🟠🔴
Síťová zařízení (např. routery, switche, firewally, access pointy)	Reset konfigurace, reset zařízení do továrního nastavení 🟢	Přepsání dat, bezpečné vymazání úložiště vhodným nástrojem 🟢🟡🟠	Mechanické zničení zařízení nebo nosiče dat 🟢🟡🟠🔴
Virtuální úložiště a cloudové služby pod kontrolou organizace	Smazání dat z úložiště 🟢	Přepsání dat, bezpečné vymazání úložiště vhodným nástrojem 🟢🟡🟠	Mechanické zničení zařízení nebo nosiče dat 🟢🟡🟠🔴

Technická aktiva mimo kontrolu organizace	Pokud jsou informace nebo nosiče mimo přímou kontrolu organizace (např. u dodavatele), musí být způsob likvidace stanoven smluvně a odpovídat úrovni aktiva.		
	Požadavek na dodavatele, aby data smazal běžným způsobem 	Dodavatel provede dokumentované přepsání dat nebo kryptografické smazání 	Certifikovaná likvidace nosiče dodavatelem s protokolem 

Uvedené příklady představují typické způsoby realizace jednotlivých metod likvidace. Organizace mohou použít i jiné postupy, pokud odpovídají definici dané metody a úrovni aktiva podle přílohy č. 1 VBO-V.

Podmínky využití informací

Využití poskytnutých informací probíhá v souladu s metodikou Traffic Light Protocol (TLP). Informace je označena příznakem, jenž určí podmínky použití informace. Jsou stanoveny následující příznaky s uvedením charakteru informace a podmínkami jejich použití:

Barva	Podmínky použití
TLP:RED	Informace nemůže být poskytnuta jiné osobě než té, které byla informace určena, nebudou-li výslovně stanoveny další osoby, kterým lze takovou informaci poskytnout. V případě, že příjemce považuje za důležité informaci poskytnout dalším subjektům, lze tak učinit pouze se souhlasem původce informace.
TLP:AMBER+STRICT	Informace může být sdílena pouze v rámci organizace příjemce, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:AMBER	Informace může být sdílena v rámci organizace příjemce a jejím partnerům, a to pouze osobám, které splňují need-to-know a jejichž informování je důležité pro vyřešení problému či hrozby uvedené v informaci.
TLP:GREEN	Informace může být sdílená v rámci organizace příjemce a případně také s dalšími partnerskými subjekty příjemce, avšak nikoli skrze veřejně dostupné kanály; příjemce musí při předání zajistit důvěrnost komunikace.
TLP:CLEAR	Informace může být dále poskytována a šířena bez omezení. Případné omezení na základě práva duševního vlastnictví původce a/nebo příjemce či třetích stran nejsou tímto ustanovením dotčena.

Verze dokumentu			
datum	**verze**	**změněno**	**popis změny**
25. května 2026	1.0	OK	Vytvoření dokumentu