PŘÍLOHA 3: ZJEDNODUŠENÁ DOPADOVÁ TABULKA

Jednotlivé oblasti, dle kterých je nutné provádět hodnocení, je možné sloučit do kategorií. Tyto kategorie by měly zahrnovat oblasti, které spolu úzce souvisí a v maximální možné míře se překrývají.

Vytvoření kategorií má sloužit k tomu, aby zrychlilo proces hodnocení tam, kde posuzované oblasti splývají, ne aby došlo k degradaci procesu hodnocení primárních aktiv a případnému vynechání některých oblastí. **Kategorie se mohou u různých organizací lišit a vždy je potřeba dopadovou tabulku přizpůsobit konkrétnímu prostředí organizace.**

Pro potřeby modelové organizace byly všechny oblasti zahrnuty v jedné z pěti kategorií.

Kategorie osobních údajů (VKB § 4 písm. a))

V rámci této kategorie se posuzuje rozsah a důležitost:

- osobních údajů s dopadem na subjekt údajů,
- finanční újma subjektu osobních údajů,
- zvláštních kategorií osobních údajů.

Kategorie povinností (VKB § 4 písm. a), b); trestně-právní řízení je nad rámec VKB)

V rámci této kategorie se posuzuje rozsah dotčených:

- právních povinností,
- obchodní tajemství,
- trestně-právní řízení,
- jiných závazků.

Kategorie chodu organizace (VKB § 4 písm. c), f), j))

V rámci této kategorie se posuzuje rozsah:

- narušení řídicích činností,
- narušení kontrolních činností,
- narušení běžných činností,
- dopadů na interní uživatele IS.

Kategorie image organizace (VKB § 4 písm. d), g), i))

V rámci této kategorie se posuzují:

- veřejné zájmy,
- obchodní a ekonomické zájmy,
- možné finanční ztráty (včetně ušlého zisku),
- zachování dobré pověsti včetně pověsti v zahraničí,
- mezinárodní spolupráce.

Kategorie core business (VKB § 4 písm. e), h))

V rámci této kategorie se posuzují dopady na:

- poskytování důležitých služeb,
- bezpečnost a zdraví osob,
- zainteresované strany (včetně externích uživatelů).

Pro modelovou organizaci byla vytvořena následující zjednodušená dopadová tabulka:

Tabulka 1: Zjednodušená dopadová tabulka

Úroveň		Kategorie osobních údajů	Kategorie povinností	Kategorie chodu organizace	Kategorie image organizace	Kategorie core business
		(sl. D, E)	(sl. F, G, Q)	(sl. H, L, P)	(sl. I, J, M, O)	(sl. K, N)
1	nízká	Může vést k **nepohodlí subjektu osobních údajů** (podrážděnost, krátkodobé časové nároky pro opětovné zadávání údajů, nutnost další komunikace s organizací). *Žádné vodítko pro finanční újmu.*	*Žádné vodítko pro zákonné a smluvní povinnosti ani pro obchodní tajemství ani pro trestně právní řízení.*	*Žádné vodítko pro narušení vnitřních řídících a kontrolních činností.* Dochází nanejvýše ke **zvýšeným časovým nárokům při provádění běžných činností**, opravu lze zajistit cca do 1 týdne. Může způsobit **krátkodobé nepříjemnosti při používání IS nebo KS** (zdržení a podráždění uživatelů, jiné zdravotní dopady na uživatele nehrozí).	*Žádné vodítko pro veřejný pořádek.* Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace) nebo může **negativně ovlivnit vztahy** s jinými částmi organizace nebo s několika jedinci veřejnosti. Negativní publicita bude ale omezena na **bezprostřední okolí a nebude mít dlouhé trvání.** Např. pro osobní údaje – nepříjemnosti s klienty, nutnost jednání s dalšími klienty, nutnost jednání s dalšími subjekty, negativní někdy i veřejná reakce subjektů údajů apod. Může mít **negativní vliv na spolupráci organizace** se zahraniční společností. Např. pro osobní údaje – může vyvolat nutnost jednání mezi organizací a zahraničním partnerem o charakteristikách zpracování osobních údajů.	Může způsobit **drobné komplikace pro malé množství osob** při zajišťování nezbytných nebo základních služeb. *Žádné vodítko pro bezpečnost a zdraví osob.*
2	střední	Může vést k **menší újmě subjektu osobních údajů** (stres, nepohodlí, drobné fyzické obtíže, nedostatek porozumění, omezení přístupu ke službám organizace nebo jiných subjektů, časové nároky spojené s řešením dopadů). Odhadovaná **finanční újma do 5000 Kč/subjekt údajů**.	Může mít **negativní dopad na skutečnosti obchodní, výrobní či technické povahy** související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu. Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností, např. provozní důvody, nedostatek zaměstnanců. Může vytvořit **podmínky pro páchání trestné činnosti** nebo může **ztížit její vyšetřování**.	Může mít **negativní dopad** na řídící a kontrolní činnosti organizace. Může **omezit provádění** běžných činností, **narušit řádné řízení nebo fungování** části nebo celé organizace, oprava vyžádá víc jak týden a méně než měsíc práce. Může **negativně ovlivnit výkon činnosti** interního nebo externího uživatele IS nebo KS (např. zvýšené časové nároky, stres uživatelů, drobné fyzické a zdravotní obtíže uživatelů).	Může zapříčinit rozsahem, formou nebo místem **omezené protesty (lokální nepokoje)**. Může přímo nebo nepřímo vést ke **ztrátám mezi 0,05 % a 2 % ročního rozpočtu**, popř. obratu organizace (v závislosti na typu organizace). Může **negativně ovlivnit vztahy** s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat **omezené zájmové skupiny nebo bude široká, avšak krátkodobá.** Např. pro osobní údaje – úbytek klientů o 10 % u organizace, krátkodobé omezení přístupu ke službám využívaným správcem, negativní, avšak krátkodobé ohlasy v médiích. Může vytvářet **negativní obraz organizace v jednom teritoriu**, **popř. v jednom státě.** Např. pro osobní údaje – může vést k dočasnému omezení zahraniční participace na zpracování osobních údajů.	Může způsobit **omezení či narušení** nezbytných nebo základních služeb pro **malé množství osob**, může způsobit **krátkodobý výpadek** služeb organizace. Může způsobit **méně závažné finanční ztráty**. Může vést **k újmě** (ohrožení osobní bezpečnosti, svobody nebo zranění) **jedné nebo několika osob**.
3	vysoká	Může vést k **závažné újmě subjektu osobních údajů** (napadení, nepříznivý zdravotní stav, deprese, ztížené uplatnění, ekonomické znevýhodnění (černé listiny), krádež identity,	Může mít **podstatný dopad** na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu.	Může mít **podstatný dopad** na řídící a kontrolní činnosti organizace a zapříčinit **dočasné zastavení chodu či podstatný zásah do fungování** organizace, **významné finanční ztráty**	Může zapříčinit rozsahem, formou nebo místem **omezené protesty na úrovni významné části správního území ORP** (obce s rozšířenou působností), jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje. Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu	Může způsobit **závažné omezení či narušení** nezbytných nebo základních služeb **pro větší množství osob, omezení nebo krátkodobé zastavení přístupu** ke službám.

Úroveň		Kategorie osobních údajů	Kategorie povinností	Kategorie chodu organizace	Kategorie image organizace	Kategorie core business
		(sl. D, E)	(sl. F, G, Q)	(sl. H, L, P)	(sl. I, J, M, O)	(sl. K, N)
		předvolání vyšetřujícími orgány). Odhadovaná **finanční újma od 5000 Kč do 50 000 Kč/subjekt údajů** (zneužití finančních prostředků subjektu údajů, poškození majetku).	Může **zapříčinit správní nebo občanskoprávní řízení** vedoucí k pokutě nebo k náhradě škody. Může vést k **narušení vyšetřování** trestné činnosti nebo soudního řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	související s obnovením chodu, oprava si vyžádá 1-2 měsíce práce. Může způsobit dočasné zastavení nebo **podstatné narušení** běžných činností organizace nebo **poškodit rozvoj** nebo prosazování cílů a zájmů organizace. Může způsobit **závažné krátkodobé omezení výkonu** činnosti interního nebo externího uživatele IS nebo KS (zhoršení zdravotního stavu uživatelů, krátkodobá pracovní neschopnost, uživatelů).	organizace (v závislosti na typu organizace). Může **závažně ovlivnit vztahy** s jinými organizacemi nebo veřejností s následkem **celostátní negativní publicity**. Např. pro osobní údaje – úbytek klientů 10-50 % u organizace, **masivní negativní, avšak krátkodobé ohlasy v médiích**. Může vytvářet **negativní obraz organizace ve světě** Např. pro osobní údaje – může být spojené dlouhodobým omezením participace zahraničních partnerů na zpracování osobních údajů.	Může vést k **újmě** (ohrožení osobní bezpečnosti, svobody nebo zranění) **větší skupiny osob, nebo ohrožení na životě jednotlivců**.
4	**kritická**	Může vést k **velmi vážné újmě subjektu osobních údajů, přímému ohrožení či ztrátě života** (smrt, invalidita, dlouhodobě nepříznivý zdravotní stav a pracovní neschopnost, ztráta zaměstnání, velmi ztížené uplatnění, vyloučení, omezení práv). Odhadovaná **finanční újma od 50 000 Kč/subjekt** údajů (neschopnost splácet dluh, ztráta majetku).	Může mít **závažný dopad** na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu. Může zapříčinit porušení právních předpisů vedoucí k **zahájení trestního stíhání**. Může vést k **závažnému, dlouhodobému narušení** schopnosti vyšetřovat trestnou činnost, popřípadě **zpochybnění soudních řízení a rozhodnutí** (závažná kriminalita, celkové zpochybnění systému).	Může mít **závažný dopad** na řídicí a kontrolní činnosti a **zapříčinit dlouhodobé zastavení chodu** celé organizace. Může způsobit **dlouhodobé zastavení běžných činností** organizace. Může zapříčinit **závažné dlouhodobé omezení výkonu činnosti** interních nebo externích uživatelů IS nebo KS (útoky na uživatele, odchod zaměstnanců, dlouhodobá pracovní neschopnost uživatelů, úmrtí).	Může zapříčinit **hromadné nepokoje**, např. generální stávku, nebo jinak závažně narušit veřejný pořádek **s celostátními dopady**. Může přímo nebo nepřímo vést ke **ztrátám přesahujícím 10 % ročního rozpočtu,** popř. obratu organizace (v závislosti na typu organizace). Může **závažně a dlouhodobě ovlivnit vztahy** s jinými organizacemi nebo veřejností s následkem **celostátní či nadnárodní negativní publicity**, **s dlouhodobými účinky** a požadavky přijetí politické odpovědnosti. Např. pro osobní údaje – úbytek klientů nad 50 % u organizace, černé listiny, ztráta konkurenceschopnosti, **masivní negativní dlouhodobé ohlasy v médiích včetně zahraničních**. Může **negativně ovlivnit nebo poškodit diplomatické vztahy** a tím způsobit nevýhodu pro zájmy ČR. Např. pro osobní údaje – dlouhodobé nebo trvalé omezení participace zahraničních subjektů nebo i států na zpracování osobních údajů.	Může způsobit **rozsáhlé dlouhodobé omezení**, **narušení či nedostupnost** poskytování nezbytných nebo základních služeb **pro větší množství osob**, **může způsobit újmu** (např. soudní proces, likvidace, vznik nesplatitelného dluhu). Může vést k **přímému ohrožení či ztrátě života** osob.
Popis kategorie		Jakékoliv informace týkající se identifikované či identifikovatelné fyzické osoby, citlivé osobní údaje.	Nutnost řídit se právními předpisy. Narušení primárních aktiv ovlivní trestně-právní řízení.	Narušení rozhodovacích možností. Znemožnění výkonu činnosti interním i externím uživatelům.	Zajištění důležitých externích informací týkající se organizace např. od EU, regulátora atd. Narušení agendy organizace. Negativní ovlivnění reputace u jednotlivců, organizačních součástí organizace, veřejnosti nebo	Narušení klíčových informací, procesů a služeb tvořící hodnotu nebo užitek organizace. Týká se systémů s dopadem na

Úroveň	Kategorie osobních údajů	Kategorie povinností	Kategorie chodu organizace	Kategorie image organizace	Kategorie core business
	(sl. D, E)	(sl. F, G, Q)	(sl. H, L, P)	(sl. I, J, M, O)	(sl. K, N)
			Narušení nezbytných provozních činností.	ostatních organizací. V případě mezinárodní spolupráce se jedná o rizika spojená s vytvořením negativního obrazu na Českou republiku u EU, NATO nebo dalších zahraničních zemí a mezinárodních organizací.	bezpečnost a zdraví osob (např. nemocnice, chemická továrna apod.).
Příklad	Únik osobních údajů fyzické osoby. Pozměnění údajů fyzické osoby. Nedostupnost osobních údajů fyzické osoby.	Narušení povinnosti zveřejňovat dokumenty na elektronické úřední desce, která je nepřetržitě dostupná vzdáleným přístupem. Vyzrazení informací v rámci trestního řízení, čímž by mohlo být trestní řízení zastaveno. Porušení mlčenlivost podle smlouvy XY a z ní plynoucí sankce. Únik podkladů potřebných pro certifikaci, které obsahují obchodní tajemství žadatelů. Ministerstvo vydá certifikát špatnému žadateli v důsledku narušení integrity dat, čímž poruší legislativu, a to může vyústit v sankce nebo žalobu od žadatele.	Neúplnost či modifikace informací potřebných pro rozhodování vedení a kontrolní činnost vede k omezení chodu organizace. Narušení činností personálních, ekonomických, správy budov a autoparku, neschopnost přijímat datové zprávy apod. Ztrátu možnosti přístupu uživatele ke službě vlivem její nedostupnosti. Neschopnost přijímat žádosti o certifikaci. Nemožnost zpracovávat informace potřebné k procesu certifikace. Nedostupnost informací o fakturách na základě nedostupnosti ekonomického systému.	Nedostupnost informací o možných obchodních příležitostech a z toho plynoucí ušlý zisk. Nedostupnost např. webu, může vést k neinformování veřejnosti o důležitých skutečnostech (např. záplavy, ekologické katastrofy atd.). Nedodržení závazků. Únik interních informací. Únik informací od zahraničních partnerů. V případě narušení bezpečnosti ztráta důvěryhodnosti.	Narušení (důvěrnosti, integrity, dostupnosti) informací, procesů a služeb vztažených směrem k hlavnímu business cíli (účelu existence) organizace (např. v případě Ministerstva pro certifikaci senzorů by se jednalo o narušení vydávání certifikací). Vydání certifikace závadnému senzoru na základě nesprávných informací, který způsobí požár.