

## 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** (Příloha č. 1, Tab. č. 4 písm. a) vyhlášky)

V rámci této kategorie se posuzuje rozsah a důležitost:

- Osobních údajů s dopadem na subjekt údajů
- Finanční újmy subjektu osobních údajů
- Zvláštních kategorií osobních údajů

**Kategorie povinností** (Příloha č. 1, Tab. č. 4 písm. a), b) vyhlášky; trestně-právní řízení je nad rámec vyhlášky)

V rámci této kategorie se posuzuje rozsah dotčených:

- Právních povinností
- Obchodních tajemství
- Trestně-právních řízení
- Jiných závazků

**Kategorie chodu organizace** (Příloha č. 1, Tab. č. 4 písm. c), f), h) vyhlášky)

V rámci této kategorie se posuzuje rozsah:

- Narušení řídicích činností
- Narušení kontrolních činností
- Narušení běžných činností
- Dopadů na interní uživatele IS

**Kategorie image organizace** (Příloha č. 1, Tab. č. 4 písm. d), g), i) vyhlášky)

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** (Příloha č. 1, Tab. č. 4 písm. e), h) vyhlášky)

V rámci této kategorie se posuzují dopady na:

- Poskytování důležitých služeb

- Bezpečnost a zdraví osob
- Zainterесované 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                                                                                                                                                                                                                                                                                                                 |
|--------|---------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 1      | nízká   | Může vést k <b>nepohodlí subjektu osobních údajů</b> (podrážděnost, krátkodobé časové nároky pro opětovné zadávání údajů, nutnost další komunikace s organizací).<br><br>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 řídicích a kontrolních činností. Dochází nanejvýše ke <b>zvýšeným časovým nárokům při provádění běžných činností</b> , opravu lze zajistit cca do 1 týdne. Může způsobit <b>krátkodobé nepříjemnosti při používání IS nebo KS</b> (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 <b>negativně ovlivnit vztahy</b> s jinými částmi organizace nebo s několika jedinci veřejnosti. Negativní publicita bude ale omezena na <b>bezprostřední okolí a nebude mít dlouhé trvání</b> . 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 <b>negativní vliv na spolupráci organizace</b> se zahraniční společností. Např. pro osobní údaje – může vyvolat nutnost jednání mezi organizací a zahraničním partnerem o charakteristikách zpracování osobních údajů.                       | Může způsobit <b>drobné komplikace pro malé množství osob</b> při zajišťování nezbytných nebo základních služeb. Žádné vodítko pro bezpečnost a zdraví osob.                                                                                                                                                                            |
| 2      | střední | Může vést k <b>menší újmě subjektu osobních údajů</b> (stres, nepohodlí, drobné fyzické obtíže, nedostatek porozumění, omezení přístupu ke službám organizace nebo jiných subjektů, časové nároky spojené s řešením dopadů). Odhadovaná <b>finanční újma do 5000 Kč/subjekt údajů</b> . | Může mít <b>negativní dopad na skutečnosti obchodní, výrobní či technické povahy</b> 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 <b>podmínky pro páchání trestné činnosti</b> nebo může <b>ztížit její vyšetřování</b> . | Může mít <b>negativní dopad</b> na řídicí a kontrolní činnosti organizace. Může <b>omezit provádění běžných činností, narušit řádné řízení nebo fungování</b> části nebo celé organizace, oprava vyžádá víc jak týden a méně než měsíc práce. Může <b>negativně ovlivnit výkon činnosti</b> 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 <b>omezené protesty (lokální nepokoje)</b> . Může přímo nebo nepřímo vést ke <b>ztrátám mezi 0,05 % a 2 % ročního rozpočtu</b> , popř. obratu organizace (v závislosti na typu organizace). Může <b>negativně ovlivnit vztahy</b> s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat <b>omezené zájmové skupiny nebo bude široká, avšak krátkodobá</b> . Např. ve vztahu k osobním údajům – úbytek klientů o 10 % u organizace, krátkodobé omezení přístupu ke službám využívaným správcem, negativní, avšak krátkodobé ohlasy v médiích. Může vytvářet <b>negativní obraz organizace v jednom teritoriu, popř. v jednom státě</b> . Např. pro osobní údaje – může vést k dočasnému omezení zahraniční participace na zpracování osobních údajů. | Může způsobit <b>omezení či narušení</b> nezbytných nebo základních služeb pro <b>malé množství osob</b> , může způsobit <b>krátkodobý výpadek</b> služeb organizace. Může způsobit <b>méně závažné finanční ztráty</b> . Může vést k <b>újmě</b> (ohrožení osobní bezpečnosti, svobody nebo zranění) <b>jedné nebo několika osob</b> . |

|   |          |                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                                                                                                                                     |
|---|----------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 3 | vysoká   | <p>Může vést k <b>závažné újmě subjektu osobních údajů</b> (napadení, nepříznivý zdravotní stav, deprese, ztížené uplatnění, ekonomické znevýhodnění (černé listiny), krádež identity, předvolání vyšetřujícími orgány).</p> <p>Odhadovaná <b>finanční újma od 5000 Kč do 50 000 Kč/subjekt údajů</b> (zneužití finančních prostředků subjektu údajů, poškození majetku).</p> | <p>Může mít <b>podstatný dopad</b> na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu.</p> <p>Může <b>zapříčinit správní nebo občanskoprávní řízení</b> vedoucí k pokutě nebo k náhradě škody.</p> <p>Může vést k <b>narušení vyšetřování</b> trestné činnosti nebo soudního řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).</p>                                                | <p>Může mít <b>podstatný dopad</b> na řídicí a kontrolní činnosti organizace a zapříčinit <b>dočasné zastavení chodu či podstatný zásah do fungování</b> organizace, <b>významné finanční ztráty</b> související s obnovením chodu, oprava si vyžádá 1-2 měsíce práce.</p> <p>Může způsobit dočasné zastavení nebo <b>podstatné narušení</b> běžných činností organizace nebo <b>poškodit rozvoj</b> nebo prosazování cílů a zájmů organizace.</p> <p>Může způsobit <b>závažné krátkodobé omezení výkonu</b> činnosti interního nebo externího uživatele IS nebo KS (zhoršení zdravotního stavu uživatelů, krátkodobá pracovní neschopnost, uživatelů).</p> | <p>Může zapříčinit rozsahem, formou nebo místem <b>omezené protesty na úrovni významné části správního území ORP</b> (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 organizace (v závislosti na typu organizace).</p> <p>Může <b>závažně ovlivnit vztahy</b> s jinými organizacemi nebo veřejností s následkem <b>celostátní negativní publicity</b>. Např. pro osobní údaje – úbytek klientů 10-50 % u organizace, <b>masivní negativní, avšak krátkodobé ohlasy v médiích</b>. Může vytvářet <b>negativní obraz organizace ve světě</b> ve vztahu k nakládání s osobními údaji – může být spojené dlouhodobým omezením participace zahraničních partnerů na zpracování osobních údajů.</p>                                                                                                     | <p>Může způsobit <b>závažné omezení či narušení</b> nezbytných nebo základních služeb <b>pro větší množství osob, omezení nebo krátkodobé zastavení přístupu</b> ke službám.</p> <p>Může vést k <b>újmě</b> (ohrožení osobní bezpečnosti, svobody nebo zranění) <b>větší skupiny osob, nebo ohrožení na životě jednotlivců</b>.</p> |
| 4 | kritická | <p>Může vést k <b>velmi vážné újmě subjektu osobních údajů, přímému ohrožení či ztrátě života</b> (smrt, invalidita, dlouhodobě nepříznivý zdravotní stav a pracovní neschopnost, ztráta zaměstnání, velmi ztížené uplatnění, vyloučení, omezení práv).</p> <p>Odhadovaná <b>finanční újma od 50 000 Kč/subjekt údajů</b> (neschopnost splácet dluh, ztráta majetku).</p>     | <p>Může mít <b>závažný dopad</b> na skutečnosti obchodní, výrobní či technické povahy související s podnikem, které mají skutečnou nebo alespoň potenciální materiální či nemateriální hodnotu.</p> <p>Může zapříčinit porušení právních předpisů vedoucí k <b>zahájení trestního stíhání</b>.</p> <p>Může vést k <b>závažnému, dlouhodobému narušení</b> schopnosti vyšetřovat trestnou činnost, popřípadě <b>zpochybnění soudních řízení a rozhodnutí</b> (závažná kriminalita, celkové zpochybnění systému).</p> | <p>Může mít <b>závažný dopad</b> na řídicí a kontrolní činnosti a <b>zapříčinit dlouhodobé zastavení chodu</b> celé organizace.</p> <p>Může způsobit <b>dlouhodobé zastavení běžných činností</b> organizace.</p> <p>Může zapříčinit <b>závažné dlouhodobé omezení výkonu činnosti</b> interních nebo externích uživatelů IS nebo KS (útoky na uživatele, odchod zaměstnanců, dlouhodobá pracovní neschopnost uživatelů, úmrtí).</p>                                                                                                                                                                                                                        | <p>Může zapříčinit <b>hromadné nepokoje</b>, např. generální stávkou, nebo jinak závažně narušit veřejný pořádek <b>s celostátními dopady</b>.</p> <p>Může přímo nebo nepřímo vést ke <b>ztrátám přesahujícím 10 % ročního rozpočtu</b>, popř. obratu organizace (v závislosti na typu organizace).</p> <p>Může <b>závažně a dlouhodobě ovlivnit vztahy</b> s jinými organizacemi nebo veřejností s následkem <b>celostátní či nadnárodní negativní publicity, s dlouhodobými účinky</b> a požadavky přijetí politické odpovědnosti. Např. pro osobní údaje – úbytek klientů nad 50 % u organizace, černé listiny, ztráta konkurenceschopnosti, <b>masivní negativní dlouhodobé ohlasy v médiích včetně zahraničních</b>. Může <b>negativně ovlivnit nebo poškodit diplomatické vztahy</b> 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.</p> | <p>Může způsobit <b>rozsáhlé dlouhodobé omezení, narušení či nedostupnost</b> poskytování nezbytných nebo základních služeb <b>pro větší množství osob, může způsobit újmu</b> (např. soudní proces, likvidace, vznik nesplátnelného dluhu). Může vést k <b>přímému ohrožení či ztrátě života</b> osob.</p>                         |

# INTERNÍ TLP:GREEN

|                            |                                                                                                              |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |                                                                                                                                                                                                                                                                                                                                                                                                                                               |                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------|--------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Popis<br/>kategorie</b> | Jakékoliv informace týkající se identifikované či identifikovatelné fyzické osoby, citlivé osobní údaje.     | Nutnost řídit se právními předpisy.<br>Narušení primárních aktiv ovlivní trestně-právní řízení.                                                                                                                                                                                                                                                                                                                                                                                                                                         | Narušení rozhodovacích možností.<br>Znemožnění výkonu činnosti interním i externím uživatelům.<br>Narušení nezbytných provozních činností.                                                                                                                                                                                                                                                                                                                                                                                     | Zajištění důležitých externích informací týkajících se organizace např. od EU, regulátora atd.<br>Narušení agendy organizace.<br>Negativní ovlivnění reputace u jednotlivců, organizačních součástí organizace, veřejnosti nebo ostatních organizací.<br>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. | Narušení klíčových informací, procesů a služeb tvořících hodnotu nebo užitek organizace.<br>Týká se systémů s dopadem na bezpečnost a zdraví osob (např. nemocnice, chemická továrna apod.).                                                                                                                                                         |
| <b>Příklad</b>             | 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.<br>Narušení činností personálních, ekonomických, správy budov a autoparku, neschopnost přijímat datové zprávy apod.<br>Ztrátu možnosti přístupu uživatele ke službě vlivem její nedostupnosti.<br>Neschopnost přijímat žádosti o certifikaci.<br>Nemožnost zpracovávat informace potřebné k procesu certifikace.<br>Nedostupnost informací o fakturách na základě nedostupnosti ekonomického systému. | Nedostupnost informací o možných obchodních příležitostech a z toho plynoucí ušlý zisk.<br>Nedostupnost např. webu, může vést k neinformování veřejnosti o důležitých skutečnostech (např. záplavy, ekologické katastrofy atd.).<br>Nedodržení závazků.<br>Únik interních informací.<br>Únik informací od zahraničních partnerů.<br>V případě narušení bezpečnosti ztráta důvěryhodnosti.                                                     | Narušení (důvěrnost, integrita, dostupnost) 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).<br>Vydání certifikace závadnému senzoru na základě nesprávných informací, který způsobí požár. |