Příloha 1

Národní úřad pro kybernetickou a informační bezpečnost — NÚKIB

Regulace odpovídající úrovni dopadu	Úroveň dopadu		Vodítka (kategorie) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita) - NUKIB v1.0 / 23.02.2018									
			A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Zákonné a smluvní povinnosti	D. Trestně-právní řízení	E. Veřejný pořádek	F. Mezinárodní vztahy	G. Řízení a provoz organizace	H. Ztráta důvěryhodnosti	I. Finanční ztráty	J. Zajišťování nezbytných služeb
Ostatní, ISVS, GDPR	1	nízká	*žádné vodítko*	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	Může narušit řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	*žádné vodítko*
Ostatní, ISVS, GDPR	2	střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS	3	vysoká *	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Může vést k narušení vyšetřování trestné činnosti nebo soudní řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	Může zapříčínit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může vytvářet negativní obraz ČR ve světě.	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	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). Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25 000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví viz vyhláška č. 437/2017 Sb.).
ZKB - KII, ISZS	4	kritická **	Může vést k přímému ohrožení či ztrátě života skupiny osob.	*žádné vodítko*	*žádné vodítko*	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	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.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě KII je hranice ztráty stanovena na 0,5% HDP.	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.
ZUI			Narušení bezpečnosti informací v oblasti "důvěrnosti" může způsobit újmu zájmům České republiky anebo nevýhodnost pro zájmy České republiky a zároveň je informace typově uvedena v seznamu utajovaných informací (§ 2 písm. a) zákona č. 412/2005 Sb.). Na základě tohoto dopadu by se za splnění dalších legislativně stanovených podmínek mělo jednat o utajované informace. Pro určení odpovídajícího stupně utajení je třeba postupovat v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. A to za splnění dalších stanovených podmínek, např. uvedených v nařízení vlády č. 522/2005 Sb.									

** V případě, že je v některém z parametrů bezpečnosti (dostupnost, důvěrnost, integrita) dosaženo max. úrovně dopadu "Vysoká", měl by správce zvážit zařazení informačního systému mezi významné informační systémy (VIS), případně mezi informační systémy základní služby (ISZS).*
- Podmínkou pro zařazení systému mezi VIS je současné naplnění definice v § 2 písm. d) zákona č. 181/2014 Sb., a alespoň jednoho oblastního kritéria podle přílohy č. 2 k vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a zároveň alespoň jednoho dopadového kritéria uvedeného v § 4 vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
- Podmínkou zařazení systému mezi ISZS je naplnění definice v § 2 písm. i) a j) zákona č. 181/2014 Sb., a současné naplnění odvětvových kritérií a alespoň jednoho dopadového kritéria uvedeného v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

*** V případě, že je v některém z parametrů bezpečnosti dosaženo úrovně dopadu "Kritická", měl by správce zvážit zařazení informačního nebo komunikačního systému mezi prvky kritické informační infrastruktury (KII), případně mezi informační systémy základní služby (ISZS).*
- Podmínkou zařazení systému mezi KII je současné naplnění definice v § 2 písm. b) zákona č. 181/2014 Sb., a alespoň jednoho odvětvového kritéria v odvětví VI., oblasti G. Kybernetická bezpečnost podle přílohy k nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury a zároveň alespoň jednoho průřezového kritéria uvedeného v § 1 nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.
- Podmínkou zařazení systému mezi ISZS je naplnění definice v § 2 písm. i) a j) zákona č. 181/2014 Sb., a současné naplnění odvětvových kritérií a alespoň jednoho dopadového kritéria uvedeného v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

Poznámka ke sloupci „Ochrana osobních údajů“:
Požadavky na zpracování osobních údajů v cloudových službách musí dle nařízení GDPR vycházet z hodnocení rizik daného scénáře zpracování pro práva a svobody fyzických osob. V případě zjištění vysokého rizika budou správci povinni provést tzv. „posouzení vlivu zpracování dat na ochranu osobních údajů“ (DPIA, viz čl. 35), a zajistit adekvátní bezpečnostní opatření a mechanismy ochrany. Přitom předpokládáme využití některého ze schválených „kodexů chování“ (viz čl. 40 GDPR) daným zpracovatelem a jeho cloudovou službou. Regulátor (ÚOOÚ) očekává, že do doby účinnosti nařízení GDPR bude schváleno několik kodexů chování, které vytvoří vhodný rámec standardizace pro vyšší úrovně dopadů zpracování osobních údajů.

Seznam použitých zkratek:
GDPR - nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
ISVS - zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
ISZS - informační systém základní služby podle § 2 písm. j) zákona č. 181/2014 Sb.
KII - kritická informační infrastruktura podle § 2 písm. b) zákona č. 181/2014 Sb.
PZS - provozovatel základní služby podle § 2 písm. k) zákona č. 181/2014 Sb.
ÚOOÚ - Úřad pro ochranu osobních údajů
VIS - významný informační systém podle § 2 písm. d) zákona č. 181/2014 Sb.
ZKB - zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
ZUI - zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti